PERSONAL DATA
PROTECTION SERVICE

JOURNAL OF PERSONAL DATA PROTECTION LAW

№ 1-2, 2025

Journal of Personal Data Protection Law

№1-2, 2025

P-ISSN 2720-8745
E-ISSN 2720-8761

The combined edition of the fifth and sixth issues of the Journal of Personal Data Protection Law is dedicated to the 33rd European Conference of Data Protection Authorities (Spring Conference) and the 75th meeting of the International Working Group on Data Protection in Technology ("Berlin Working Group", IWGDPT)

Table of Contents

From the Editor-in-Chief

Dear Reader,

We are pleased to present the combined first and second editions of the Journal of Personal Data Protection Law for the current year, dedicated to the 33rd European Conference of Data Protection Authorities – the Spring Conference and the 75th meeting of the International Working Group on Data Protection in Technology ("Berlin Working Group", "IWGDPT"). Notably, in the current year, the Personal Data Protection Service served as the host institution for both international events.

The 33rd European Spring Conference of Personal Data Protection Supervisory Authorities — the highest-level international event in the field of personal data protection was hosted by the Personal Data Protection Service in the city of Batumi. The Spring Conference has been held since 1991 and plays a significant role in shaping new trends in privacy and data protection. Its main objective is to foster dialogue between European data protection supervisory authorities and practitioners, thereby creating a strong forum for discussing challenges and opportunities in the field. The conference serves as a key platform for the discussion of European standards in personal data protection and the exchange of best practices.

Although personal data protection law is a relatively new field, the protection of personal space and private life has a centuries-old history. The words of Ilia Chavchavadze "A person's greatest treasure is their identity" — which served as the tagline of the conference, aptly reflect our shared values concerning personal identity and private life. Over the course of three days, participants had the opportunity to discuss with European colleagues a wide range of important issues in the field of personal data protection, including the regulation of Artificial Intelligence; legislative frameworks for data protection at the regional, European and global levels; modern technological developments and the impact of Artificial Intelligence on privacy; children's privacy; contemporary challenges related to the protection of health-related personal data and the role of personal data protection officers and privacy practitioners, among others.

The 75th meeting of the International Working Group on Data Protection in Technology, established in 1983, was hosted by the Personal Data Protection Service in Tbilisi at Ivane Javakhishvili Tbilisi State University. The meeting addressed current challenges and topical issues at the intersection of personal data protection law and technology, including neurodata, 6G technology, digital identity, and related subjects. The event was attended by twenty-five representatives from fourteen countries, as well as by the European Data Protection Supervisor ("EDPS") and the Electronic Privacy Information Center ("EPIC").

This edition of the Journal of Personal Data Protection Law brings together interventions presented within the framework of the above-mentioned international events, as well as scholarly contributions by practitioners and researchers in the field of personal data protection law. I would like to express my sincere gratitude to all participants for the submitted articles, which offer readers a unique opportunity to engage with the issues discussed at the conferences. We hope that the works published in this edition will be both of scholarly interest and of practical value, serving as a useful resource for those interested in the activities of the Personal Data Protection Service and for legal practitioners working in this field.

Dr. Dr. Lela Janashvili

President of the Personal Data Protection Service of Georgia
Associate Professor at Ivane Javakhishvili Tbilisi State University
Associate Professor at the Autonomous University of Barcelona

Sharon Azarya*

Facial Recognition Technology: Navigating Privacy Rights and Regulatory Challenges

1. Introduction

Facial recognition technology has rapidly evolved from a futuristic concept to an everyday reality, permeating both public and private sectors across the globe. While proponents highlight its potential to enhance security and streamline services, critics warn of unprecedented threats to privacy, human rights, and social equity. The International Working Group on Data Protection in Technology, commonly known as the Berlin Group, has produced a comprehensive working paper that examines these competing concerns and proposes a framework for responsible governance of this transformative technology.[1]

This article analyzes the Berlin Group's findings on facial recognition technology, exploring its technical attributes, diverse applications, inherent risks, and the regulatory approaches necessary to safeguard fundamental rights.

2. Understanding Facial Recognition Technology

Facial recognition technology operates by converting images or videos of human faces into mathematical templates that can be compared against databases of known individuals. The technology performs four basic functions: detection, verification, identification, and facial analysis.[2] Detection recognizes that a face exists in an image. Verification confirms whether a person matches a claimed identity through one-to-one matching. Identification compares an unknown face against a gallery of known individuals through one-to-many matching. Facial analysis attempts to infer characteristics from facial features, though the scientific validity of such inferences remains highly contested.

Most contemporary systems rely on machine learning algorithms trained on large datasets of facial images. As these algorithms process more training data, they theoretically become more accurate in distinguishing individuals, though accuracy encompasses multiple considerations including false positive rates, false negative rates, and performance across different demographic groups.[3]

---

* Head of the International Department in the Israeli Privacy Protection Authority.

[1] International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, 2023, 1.

[2] Ibid, 4-5.

[3] Ibid, 5-6.

3. Applications and Controversies

The Berlin Group documents an extensive range of facial recognition applications in both private and public contexts. In the private sector, the technology serves functions including secure access to premises and devices, security monitoring in venues such as casinos and retail stores, marketing and customer service applications, and attendance monitoring in workplaces.[4] However, these deployments have not proceeded without opposition. Data protection authorities in the Netherlands and Canada have deemed certain retail facial recognition systems unlawful, establishing important precedents for privacy protection.[5]

Government agencies have embraced facial recognition for border control, access to digital services, law enforcement, and educational settings.[6] Law enforcement applications present particularly acute concerns, as police agencies use facial recognition to identify uncooperative suspects, maintain mugshot databases, investigate crimes, and deploy live facial recognition systems to locate wanted individuals in real time.[7] The introduction of facial recognition in schools has proven especially contentious, with critics arguing that subjecting minors to continuous biometric surveillance may harm their development and discriminate against students with autism spectrum disorders or physical conditions affecting facial appearance.[8]

4. Privacy Risks and Fundamental Rights Implications

Facial recognition systems deployed in public spaces capture the faces of all passersby indiscriminately, creating constant and pervasive surveillance that fundamentally erodes anonymity.[9] Such systems may reveal or enable inferences about individuals' political opinions, religious beliefs, medical conditions, and sexual orientation. The mere knowledge that facial recognition systems operate may deter people from attending demonstrations, visiting places of worship, or accessing health clinics, creating a chilling effect on democratic participation.[10]

Facial recognition systems have demonstrated documented patterns of accuracy errors that disproportionately affect certain populations. Research indicates that Asian and African American individuals face up to one hundred times greater likelihood of misidentification compared to white men.[11] Women, transgender individuals, non-binary people, and individuals with certain disabilities also experience higher error rates. The Privacy Commissioner of Canada emphasizes that facial recognition accuracy must be understood statistically rather than as binary truth, with system outputs

[4] Ibid, 7-10.
[5] Ibid, 8.
[6] Ibid, 11-12.
[7] Ibid, 13-14.
[8] Ibid, 12.
[9] Ibid, 14-15.
[10] Ibid, 15.
[11] Ibid, 16.

representing probabilistic inferences about identity rather than verified facts.[12] Training data quality fundamentally shapes algorithm performance; systems trained on non-representative datasets inevitably produce disparate accuracy across demographic groups.

Certain applications present accuracy and bias problems so severe that ethical deployment becomes impossible. Emotion recognition systems presume universal emotional expression, assumptions contradicted by cross-cultural research.[13] These systems frequently assign more aggressive emotions to Black faces regardless of actual expression, perpetuating racist stereotypes. Biometric categorization systems that claim to predict sexuality, criminality, or other traits from facial features rest on premises virtually indistinguishable from discredited pseudosciences like phrenology.[14]

The permanent and unchangeable nature of facial biometric data magnifies the consequences of security breaches. Unlike passwords or credit card numbers, faces cannot be reset or replaced following data compromise.[15] Hackers gaining access to facial recognition data may steal identities, impersonate victims, or conduct illegal activities using stolen biometric identities. Major breaches have already occurred, including a Chinese database containing millions of facial records left exposed online for months.[16]

Live facial recognition technology presents additional risks beyond retrospective analysis. These systems automatically collect biometric data in real time, indiscriminately processing information about all individuals who pass through monitored areas.[17] A documented case from London illustrates potential abuse: Metropolitan Police officers stopped and questioned a fourteen-year-old schoolboy based on a false match later confirmed as non-credible.[18]

5. Regulatory Approaches and Recommendations

The Berlin Group proposes multiple strategies for mitigating facial recognition risks, ranging from outright prohibitions to technical safeguards and procedural requirements. Before implementing any system, controllers must conduct comprehensive risk assessments considering factors including the scope of individuals affected, whether data storage is centralized or decentralized, whether the system includes search capabilities, how templates are stored, whether data collection is mandatory or voluntary, the transparency and consent framework, and target environment characteristics.[19]

Many jurisdictions have concluded that certain applications pose such severe

[12] Ibid, 18-19.
[13] Ibid, 16-17.
[14] Ibid, 17-18.
[15] Ibid, 21.
[16] Ibid, 22.
[17] Ibid, 23.
[18] Ibid, 24.
[19] Ibid, 25-27.

threats to fundamental rights that outright prohibition represents the only appropriate response. The European Data Protection Board and European Data Protection Supervisor have called for a general ban on automated recognition of human features in publicly accessible spaces.[20] The European Parliament has advocated for permanent prohibition of automated individual recognition in public spaces and bans on private facial recognition databases like Clearview AI.[21] These proposals emerged following enforcement actions by data protection authorities across Europe, Australia, and Canada against companies operating facial recognition systems without adequate legal basis or safeguards.

Several U.S. jurisdictions have enacted prohibitions, with Vermont, Maine, New Hampshire, Oregon, and California restricting or banning facial recognition in various contexts.[22] Over one hundred organizations and hundreds of experts from more than forty countries have endorsed recommendations that countries suspend further deployment of facial recognition for mass surveillance pending establishment of adequate legal frameworks.[23]

Where facial recognition deployment is not categorically prohibited, clear and specific legal basis must exist for processing biometric data.[24] For high-risk deployments, organizations should consult competent data protection authorities prior to implementation. Facial recognition in public spaces must serve necessary and important public interests that cannot be protected through less invasive means.

Consent represents a problematic legal basis in many contexts due to power imbalances and the practical impossibility of meaningful consent in public spaces.[25]

The public deserves notification about facial recognition deployment in public spaces.[26] Transparency should extend to data protection impact assessments and results of accuracy and bias testing. Signage must be prominently visible before individuals enter surveilled areas and clearly indicate that facial recognition is operating.

Controllers must implement multiple technical measures to mitigate risks. Data accuracy requires optimal conditions for training datasets, comparison databases, cameras, lighting, and imaging.[27] Regular examination of datasets must ensure diversity across ages, genders, and skin tones. Controllers should establish appropriate confidence thresholds and performance metrics, discontinuing processing when systems fail to meet requirements. Where facial recognition decisions affect data subjects, final decisions must involve human intervention by well-trained professionals rather than relying on automated processing alone.[28]

[20] Ibid, 28.
[21] Ibid, 28-29.
[22] Ibid, 30.
[23] Ibid.
[24] Ibid, 30-31.
[25] Ibid, 32.
[26] Ibid.
[27] Ibid, 32-33.
[28] Ibid, 33.

Data minimization strategies should guide system design and operation.[29] Controllers should limit stored personal data, delete raw images after extracting templates when no longer required, implement automatic erasure after defined retention periods, avoid unnecessary cross-referencing with other data sources, store templates separately from identifying information, encrypt and anonymize data, and restrict data retention to periods necessary for specified purposes. Comprehensive data security measures must address vulnerabilities throughout the data flow cycle.[30]

6. Conclusion

The Berlin Group's working paper provides a rigorous framework for understanding and addressing the profound challenges facial recognition technology poses to privacy, human rights, and social equity. While acknowledging potential beneficial applications, the document makes clear that facial recognition's capacity for intrusive, arbitrary, and discriminatory surveillance demands robust regulatory responses that prioritize fundamental rights protection.

The variety of regulatory approaches emerging globally reflects ongoing societal deliberation about appropriate boundaries for biometric surveillance in democratic societies. The working paper's emphasis on comprehensive risk assessment, clear legal frameworks, meaningful transparency, accuracy accountability, and technical safeguards offers practical guidance for policymakers, data protection authorities, and deploying organizations.

Bibliography:

1. International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, 2023.

[29] Ibid, 34.
[30] Ibid, 35.

Sharon Azarya*

Data Protection and Privacy in Smart Cities: A Critical Analysis of the IWGDPT Working Paper

1. Introduction

The rapid digitalization of urban environments has transformed cities into complex ecosystems of data collection, analysis, and automated decision-making. The International Working Group on Data Protection in Technology (IWGDPT) addresses this transformation in their working paper "Smart Cities," which provides a comprehensive framework for understanding the data protection challenges inherent in smart city development.[1] This essay examines the paper's key contributions to the discourse on urban digitalization, analyzing its tripartite framework of data collection, analysis, and decision-making, while evaluating the practical implications of its recommendations for cities, industry, and regulators.

2. The Smart Cities Framework: Beyond Definitional Debates

Rather than engaging in the contentious debate over what constitutes a "smart city," the IWGDPT paper adopts a pragmatic approach by focusing on the process of digitalization itself.[2] This methodological choice represents a significant contribution to the field, as it shifts attention from abstract definitions to concrete data protection challenges. The paper's three-stage framework—data collection, data analysis, and decision—provides a structured lens through which to examine the lifecycle of data processing in urban contexts.

The data collection stage encompasses diverse technologies ranging from Internet of Things (IoT) sensor networks and CCTV systems to the reuse of data held by public authorities and municipalities.[3] The analysis stage involves sophisticated processing techniques including data matching, artificial intelligence, profiling, and the construction of digital twins—digital representations of physical cities used for policy experimentation.[4] Finally, the decision stage encompasses the application of these analytical outputs to manage city resources, control urban functions, and inform policy development. This comprehensive mapping of smart city operations provides a foundation for understanding where data protection risks emerge and how they might

* Head of the International Department in the Israeli Privacy Protection Authority.

[1] International Working Group on Data Protection in Technology, Working Paper on "Smart Cities", Adopted at the 70th Meeting on 29th-30th November 2022, Written Procedure Prior to 71st Meeting on 7th-8th June 2023, 1.

[2] Ibid.

[3] Ibid, 2.

[4] Ibid.

be mitigated.

3. Accountability and Governance: The Foundation of Ethical Smart Cities

The paper's emphasis on accountability and governance as preconditions for smart city initiatives represents its most critical contribution. The IWGDPT argues that cities must conduct rigorous accountability assessments, including data protection impact assessments, before commencing any processing activities.[5] This proactive approach challenges the common practice of retrofitting privacy protections onto existing systems—a practice that has repeatedly proven inadequate in protecting individual rights.

The concept of identifiability receives particular attention in the accountability section. The paper correctly identifies that identifiability must be assessed not only in relation to specific processing operations but also in connection with associated processing that may enable indirect identification.[6] This holistic view of identifiability reflects an understanding of the cumulative privacy risks that arise when multiple data systems operate in proximity.

The Enschede case study illustrates the consequences of inadequate accountability measures. The municipality of Enschede implemented 24/7 Wi-Fi tracking in its city center, arguing that its anonymization techniques rendered the data non-personal.[7] However, the Dutch Data Protection Authority determined that the combination of hashed MAC addresses, timestamps, and location information constituted personal data, as the anonymization method did not sufficiently exclude the risk of singling out individuals.[8] This case demonstrates the importance of rigorous pre-implementation assessment and the limitations of technical anonymization measures when applied without adequate consideration of re-identification risks.

4. Data Minimization: Reconciling Innovation with Privacy

The principle of data minimization takes on particular significance in smart city contexts, where the temptation to collect comprehensive datasets for future, undefined purposes conflicts with fundamental privacy protections. The paper argues that when trend analysis is the objective, cities should aggregate data and strip identifiers as early as possible in the collection stage.[9] This approach represents a departure from the data maximalist logic that has dominated much of the technology sector's approach to urban digitalization.

[5] Ibid, 3.
[6] Ibid, 4.
[7] Ibid, 6.
[8] Ibid.
[9] Ibid, 8.

The Transport for London (TfL) Wi-Fi data collection initiative provides a positive example of data minimization in practice. TfL sought to understand customer movement through stations without identifying specific individuals.[10] By implementing automatic hashing using revolving cryptographic functions immediately after collection, and by refraining from matching Wi-Fi data with other datasets such as travel card information, TfL demonstrated that valuable urban insights can be obtained while respecting data minimization principles.[11]

The paper's recommendation that cities embed minimization practices into collection systems through technical measures—such as procuring sensors that strip identifiers before transmission—represents an important contribution to privacy by design discourse.[12] This approach shifts responsibility for data protection from individual choice or post-collection governance to the technical architecture itself, creating systemic safeguards that persist regardless of changes in personnel or organizational priorities.

5. Purpose Limitation: Confronting Function Creep

The multifaceted roles that cities play in citizens' lives create particular challenges for purpose limitation. The paper identifies a significant risk: that data collected for one municipal function—such as traffic management—might be repurposed for another function—such as law enforcement or social benefit determination—without adequate assessment or legal basis.[13] This phenomenon, often termed "function creep," poses serious threats to individual autonomy and institutional trust.

The smart homes case study illustrates the complexity of purpose limitation in practice. When sensors installed in social housing to monitor moisture and damp levels—a maintenance purpose—are proposed for use in identifying households eligible for fuel poverty benefits—a social welfare purpose—fundamental questions of compatibility arise.[14] The paper correctly identifies that even well-intentioned interventions into individuals' lives require either clear legal authorization or valid consent when they deviate from the original purpose.[15]

The recommendation for compatibility assessments when using data for purposes other than those for which it was originally collected provides a practical framework for addressing function creep.[16] However, the paper could have provided more detailed guidance on how cities should conduct such assessments, particularly when the new purpose might be characterized as serving the public interest.

[10] Ibid.
[11] Ibid, 9.
[12] Ibid, 8.
[13] Ibid, 10.
[14] Ibid, 11.
[15] Ibid.
[16] Ibid, 12.

6. Security and Transparency: Emerging Challenges

The paper's discussion of integrity and confidentiality highlights the security vulnerabilities inherent in the proliferation of IoT devices in urban environments. The reference to emerging legislative initiatives, such as the United Kingdom's Product Security and Telecommunications Infrastructure Bill, demonstrates growing recognition of IoT security deficiencies.[17] The prohibition of default passwords, requirements for vulnerability disclosure, and mandated security update periods represent important steps toward addressing these systemic weaknesses.

The transparency recommendations are particularly noteworthy for their recognition that smart city data collection is often "passive"—occurring without individual opt-in and potentially invisible to those affected.[18] The paper's advocacy for multiple transparency mechanisms, including signage at collection points, public registers of processing activities, and algorithm registers, acknowledges that different contexts and audiences require different communication strategies.[19]

The Amsterdam Algorithm Register is cited as an innovative approach to transparency, providing a publicly accessible listing of algorithmic processing occurring in the city.[20] Such initiatives represent a significant advancement over traditional privacy notice approaches, which typically provide information only to individuals directly affected by specific processing operations. By creating city-wide transparency mechanisms, municipalities can foster broader public understanding and democratic debate about the trajectory of urban digitalization.

7. Implications and Future Directions

The IWGDPT paper provides comprehensive and valuable guidance for data protection in smart cities, establishing a solid foundation for responsible urban digitalization. The paper's structured approach and practical recommendations offer cities, industry, and regulators a clear roadmap for implementing privacy-respecting smart city initiatives.

The paper's emphasis on accountability and governance reflects a forward-thinking approach that recognizes the complexity of modern urban data ecosystems. By placing data protection considerations at the forefront of smart city planning, the framework encourages cities to adopt proactive rather than reactive approaches to privacy protection. This preventive stance has the potential to build and maintain public trust, which is essential for the long-term success of smart city initiatives.

The incorporation of real-world case studies, such as the Enschede Wi-Fi tracking and Transport for London's privacy-preserving data collection, provides practical

[17] Ibid, 13.
[18] Ibid, 14.
[19] Ibid, 15-16.
[20] Ibid, 15.

illustrations that can guide cities in their implementation efforts. These examples demonstrate both the challenges and opportunities inherent in smart city development, offering valuable lessons for municipalities at various stages of digitalization.

Looking forward, the principles outlined in this paper provide a foundation for continued dialogue and development in smart city governance. The paper's invocation of Aristotle's assertion that cities exist to grant citizens "a complete and self-sufficient life"[21] reminds us that technological advancement must ultimately serve human flourishing. As smart city technologies continue to evolve, the framework established by this paper can serve as a touchstone for ensuring that innovation proceeds in alignment with fundamental rights and democratic values.

The collaborative approach advocated by the paper—involving cities, industry, regulators, and citizens—recognizes that successful smart city development requires multi-stakeholder engagement.[22] This inclusive vision suggests that the future of smart cities will be shaped not only by technological capabilities but by collective commitment to ethical principles and human-centered design.

8. Conclusion

The IWGDPT working paper on smart cities represents a significant contribution to the literature on urban digitalization and data protection. By providing a structured framework for analyzing data flows, identifying privacy risks at each stage of processing, and offering concrete recommendations for cities, industry, and regulators, the paper advances both theoretical understanding and practical implementation of data protection in urban contexts.

The paper's emphasis on proactive accountability, data minimization, purpose limitation, and transparency provides a foundation for developing smart cities that respect individual privacy while pursuing legitimate urban management objectives. The case studies, particularly the contrasting examples of Enschede's inadequate anonymization and Transport for London's privacy-preserving approach, offer valuable lessons for municipalities embarking on digitalization initiatives.

However, as cities continue to evolve into increasingly data-intensive environments, ongoing research and policy development will be necessary to address emerging challenges. The recommendations in this paper should be viewed not as a complete solution but as an initial framework that requires continuous refinement in response to technological developments, regulatory evolution, and lived experience of smart city initiatives. The ultimate success of smart cities will depend not only on their technical sophistication but on their ability to maintain the trust and support of the citizens they serve—a goal that can only be achieved through rigorous attention to data protection and respect for fundamental rights.

[21] Ibid, 1.
[22] Ibid, 5.

Bibliography:

1. *International Working Group on Data Protection in Technology*, Working Paper on "Smart Cities", Adopted at the 70th Meeting on 29th-30th November 2022.

Norbert Bernsdorff*

The Historical Roots of Data Protection – How It Came About!

The article discusses the historical roots of data protection, which trace back literally to antiquity. It introduces the foundations of data protection terminology, early and modern-day forms of data protection and its progress throughout the years. Special emphasis is put on the emergence of data protection regulatory frameworks since 1970, from Germany to modern-time legal instruments that form the EU and Council of Europe's frameworks on data protection and privacy.

Keywords: *Roots of data protection, data protection terminology, right to privacy.*

1. Introduction

In the relevant literature, data protection is often regarded as a "discipline without history". This is not true in this exclusive sense. It is right that the modern concept of data protection legislation - meaning data protection law - as we know it today has only developed in recent decades. However, the protection of privacy has a long history. In principle, it goes back to antiquity. Nevertheless, it would be going too far to regard the fig leaf that Adam and Eve used when they were expelled from paradise as an early form of data protection. But of course, even in the earliest times, there were sanctioned forms of behavior that today would be described as personality-protecting. There was the so-called taboo and the refuge – in Latin: Refugium. The latter refers to a place of retreat, including a physical one. The second of the Ten Commandments in the Old Testament includes the so-called prohibition of images - "You shall not make thyself an image!"

* Doctor of Law, Professor at the Philipps University of Marburg; Retired judge at the Federal Social Court of Germany. Member of the Editorial Board of the Journal of Personal Data Protection Law.

2. Data Protection Terminology

Before we turn to the historical roots of data protection, its concept must be clarified!

The term data protection is actually not very useful for what it is supposed to describe. In purely linguistic terms, the word signals that it is, to a certain extent, self-reflexively about the protection of data. This, however, shortens the actual topic, because data protection is not about protecting the data itself, but rather about protecting the people behind the data. In other words, to stay in the current reality of life – as an example: corona crisis -, it is not about protecting the date "vaccinated or recovered", but about protecting the information "Mr. or Mrs. *Miller* is vaccinated or recovered". Therefore, data protection is about so-called personal data, meaning all information that can be used to identify a natural person or that can be assigned to a person. The German pioneers of data protection, *Ulrich Seidel* and *Wilhelm Steinmüller*, pointed out this accurate differentiation back in the 1970s, when data protection legislation was in the starting blocks.

3. From the Protection of Secrets to Professional Confidentiality Obligations and the Modern Right of Personality

3.1. Starting Point: Protection of Secrets in the Pre-Modern Era

Privacy as a legal category is a category from the modern era. This category is only around 100 years old. However, the origins of data protection go back much further, namely to the pre-Christian protection of secrets.

Did you know that data protection goes back to the so-called Hippocratic Oath? Back in the year 400 before Christ, doctors undertook not to divulge their patients' intimate secrets to third parties. In other words, it was about medical confidentiality, which is still practiced today. It was recognized that people would reveal more about themselves and thus make treatment easier if they could trust their doctors to "keep their mouths shut". This rule of conduct, which was described as a sacred duty at the time, was based on religious and ethical considerations.

Since the Middle Ages, sinful Catholics have also been able to count on data protection. This is because in 1215 after Christ, the so-called secrecy of the confessional was incorporated into church law. This was laid down by the heads of the Catholic Church in the most important decision-making assembly of the time - the Fourth Lateran Council. The secrecy of the confessional obliges clergymen to maintain absolute secrecy about everything entrusted to them in confession. Not even the confessing themselves can release their confessors from their duty of confidentiality. Clergymen who violate the secrecy of the confessional could and can face the worst punishment of all: expulsion from the church. An anecdote in passing: In the

confessional boxes of the Catholic Church, a rose carved out of wood reminds those present of the secrecy of the confessional: in Latin: "sub rosa dictum" - what is said under the rose must remain secret.

The so-called secrecy of correspondence, post and later telecommunications, as well as German tax secrecy, should also be included in this category of secrets - at least in Germany. Curiosity is deeply human, but not always socially acceptable. To prevent messengers from poking their noses into things that were none of their business, the General Prussian Postal Regulations of 1712 placed the secrecy of correspondence under official protection. Postal workers who violated this regulation were threatened with dismissal and criminal prosecution. The aforementioned secrets were later also included in German constitutions. Today, they are enshrined in Article 10 of the German Basic Law.

With the emergence of the modern state, it used every opportunity to comprehensively enforce its claim to power and regulation. This also applied to tax collection: In former times, citizens could not be forced to disclose tax-relevant data. In order to be able to extend the powers of intervention of tax collectors, the protection of secrets had to be expanded in parallel. To this day, this provides a protective framework for information about citizens that becomes known in the course of taxation proceedings. Tax secrecy was initially only a general - non-punishable - official secret, but later became binding. Today, tax secrecy has a significance similar to that of a fundamental right.

3.2. Obligations of Confidentiality as a Preliminary Form of Data Protection?

During my previous work as data protection officer for the judiciary in Lower Saxony, Germany, I often had to deal with the legal question of the relationship between the duty of confidentiality and data protection. Are confidentiality obligations a form of special data protection that takes precedence over general data protection regulations? Are they sector-specific data protection law?

So the question is: Are confidentiality obligations also a historical root of data protection?

The answer is: Only in part! - The general secrecy of public officials has always had a different purpose. It was never intended to protect the individual, but always existed solely to safeguard the interests of the state and the public principal. The general confidentiality obligations of public officials were therefore not a precursor to data protection.

A duty of confidentiality must be judged differently if it applies to certain professional groups: doctors, lawyers, notaries, social workers, but also data protection officers. In my view, these professional confidentiality obligations are rightly referred to as the historical prototypes of data protection.

3.3. Data Protection and Personality Rights — the Modern Era

The more time progressed, the more the modern state collected data about its population. Technical developments made this possible. Registries replaced the old archives, which at the time were merely disorganized "file graves". Collecting data on one's own population was nothing new, as we remember from the biblical Christmas story: Christ's birth was preceded by the instruction from *Emperor Augustus* that "all the world should be written down". In the Middle Ages, in order to protect security and order, systematic records were kept of the so-called traveling people, for example in *Nürnberg* as early as 1449. However, with the expansion of information technology, data collection later became more and more complete: dragnet investigations, online searches, vehicle license plate recognition, data retention, etc. The state became "Big Brother".

I don't want to go into the period of the Nazi dictatorship in Germany here. It was aimed at the complete surveillance of the population with the means available at the time. The so-called Research Office – in German: Forschungsamt - assigned to *Hermann Göring* overrode all existing secrecy obligations. A comprehensive national database was to be created in the form of a so called *German Tower* – in German: *Deutscher Turm*. Nor do I want to say anything about the data power that the former German Democratic Republic exercised over its population. The most visible sign of this are the so-called *Stasi* files, the extensive files of the East German State Security. Experts agree that both periods should be viewed separately from the perspective of data protection history.

What did data protection consist of up to this time, which means before it became the subject of legal regulations?

The answer is obvious: Until then, data protection was simply achieved through the technical limitations of data processing. Due to the lack of data storage and processing options, the state was prevented from gaining comprehensive access. Neither the Nazi dictatorship nor later the State Security of the German Democratic Republic were able to effectively monitor their populations because they lacked the information and administrative technology - thank God, one must say!

3.3.1. A New Construction Site: Information Processing by Private Actors

Until the second half of the 19th century, data collection by private actors played no role. From 1840, however, private credit agencies and detective agencies began to keep so-called black lists: 1841 - *Dun&Bradstreet*, *Florida*, 1872 - *Schimmelpfeng*, *Germany*, 1879 - *Creditreform*, *Switzerland*, 1885 - *Bürgel*, *Germany*, 1927 - *SCHUFA*, the Protection Association for General Credit Protection – in German: Schutzgemeinschaft für allgemeine Kreditsicherung. Some of the credit agencies founded at that time still exist today. Improved storage techniques, such as those associated with the name *Leitz* - everyone knows the Leitz *folders* - were helpful

As commercial players, the media and press also came into focus. Violations of personality rights led to the enactment of the German Art Copyright Act – in German: Kunsturheberrechtsgesetz - and the right to one's own image in 1907. The reason for this was a so-called paparazzo photo of the dead Imperial Chancellor – in German: Reichskanzler - *Otto von Bismarck*: Two photographers had illegally entered the death chamber, photographed the deceased and attempted to publish the images. The outrage was great. However, according to the law at the time, the two could only be convicted of trespassing. So it was decided to better protect the dignity of the deceased in future. In addition to the right to one's own image, the so-called post-mortem right of personality, meaning the protection of personality rights after death, has also been guaranteed since then.

3.3.2. Starting Point of the Modern Data Protection Debate in America Out of All Things

Would you have guessed that the roots of modern data protection lie in the United States of America? This is remarkable because it is a country that collects and processes personal data in an uncontrolled manner today. I only have to remind you of the so-called *Safe Harbor* and *Privacy Shield agreements* on data transfer there.

As early as 1890, American lawyers such as *Samuel Warren* and the later Supreme Court judge *Louis Brandeis* spoke out in favor of a right to "privacy solitude". In their groundbreaking essay "The Right to Privacy", which they published in the renowned *Harvard Law Review*, they created the "right to be left alone" as a natural right of every human being. *Vance Packard* in his 1964 book "The Naked Society" and *Alan Westin* in his 1967 work "Privacy and Freedom" expressed the same view - albeit more than 70 years later. These publications were inspired by the increasing publication of intimate details of people's private lives - a consequence of the mass circulation of newspapers and the further development of photography. Legal protection - they said - was also needed for so-called intangible property such as privacy. However, these data protection policy debates came too early for America; the first substantial result of these discussions was the Privacy Act of 1974.

The data protection debate in the United States of America was an impetus for jurisprudence in Germany!

3.3.3. "Home" of Data Protection in the General Right of Personality

While the focus in Germany was initially - in contrast to today's concept - on objective-legal restrictions on state and private data power - meaning mere program statements with an impact on state activities - these were later replaced by a subjective right to data protection: the general right of personality as a legal category. As this is neither mentioned in the German Basic Law – in German: Grundgesetz - nor

in the German Civil Code – in German: Bürgerliches Gesetzbuch -, it was developed by the courts from the beginning of the 1960s, above all by the German Federal Constitutional Court.

4. The Beginning of Data Protection Legislation — From Hessen to the World

The birthplace of global data protection legislation was - and here I can give us a pat on the back - Germany. This is the cradle of the world's first data protection law. It came into force in 1970 in the federal state of Hessen. Further data protection laws followed in Bavaria and in Rhineland-Palatinate in the year 1974.

This all happened at a time when computers were still as big as bookshelves and as powerful as today's pocket calculators. This was also the time when fiber optic cable and on-screen text on television were new. However, there were already 7,500 electronic data processing systems in Germany at the time.

The following is perhaps of particular interest to the Personal Data Protection Service here at the company: The establishment of an independent data protection officer was also a Hessian "invention". The Hessian Data Protection Act created the legal basis for this. The world's first data protection officer was called *Willi Birkelbach*; he was appointed by the Hessian state government in 1971.

After the journey had begun in the federal state of Hessen, the German legislator only followed suit around six years later and passed a data protection law for the whole of Germany in 1977.

5. December, 1983 — the So-Called Census Ruling of the German Federal Constitutional Court

I remember the protest on the streets of Germany very well. I was a student at the time. The protest was about the planned comparison of statistical data with the population registers; this comparison was to be made possible by a census starting in 1980. Posters addressed to the German state read: "Don't count us, count your days!"

The so-called census ruling by the German Federal Constitutional Court in 1983 was a sensation and paved the way for the elevation of data protection to the level of fundamental rights. Based on preliminary works by *Wilhelm Steinmüller*, whom I have already mentioned, it recognized a so-called fundamental right to informational self-determination. Two things were new: Since then, there is no longer any personal data about people that is irrelevant from the outset. In addition, all data processing is subject to the law. A new understanding of data protection law was born! From then on, the ruling was celebrated as a "stroke of genius" in data protection law, not only in Germany but also abroad.

To round things off, please allow me to make the following point: Until 2006, German citizens had no general right of access to government documents. So how

could they make use of their data protection rights if they didn't even know what data the state administration had stored about them? This changed with the so-called Freedom of Information Act – in German: Informationsfreiheitsgesetz -. It grants every person in Germany the unconditional right to view official information from all public authorities. Data protection and freedom of information are not contradictory, they are - so it is said - two sides of the same medal.

6. Data Protection Goes Europe

When did data protection law become European, you may ask? - It is above all this Europeanized data protection law that you are dealing with here in Georgia!

Well, the Council of Europe was the standard setter - long before the European Union. Its 1981 convention (ETS No. 108) was the world's first international agreement in the field of data protection. However, it only lays down minimum standards - which was intended at the time. The aforementioned convention was signed on January 28, 1981 by the then member states of the Council of Europe. This is the reason why the „European Data Protection Day“ is celebrated every year on this day. This day is today.

Since the year 1995, it is also worth taking a look at the European Union. The German, but also the French example "set a precedent" here. After the European Union was founded, it was not only goods that were able to cross internal borders unhindered, but also personal data: So a uniform minimum level of data protection had to be established. The European Union adopted the so-called Data Protection Directive 95/46/EC in 1995 and - because it wanted to separate data protection in the telecommunications sector from this in procedural terms - the so-called e-Privacy or Cookie Directive 2002/58/EC in 2002. I think you are familiar with both.

The last word in data wisdom is the European Union's well-known General Data Protection Regulation, which has been in force since 2018. Just as an aside: About ten years earlier, European data protection law had been raised to the level of fundamental rights by Article 8 of the European Charter of Fundamental Rights - a logical intermediate step! The General Data Protection Regulation lays down stricter rules for the processing of personal data and strengthens the rights of data subjects. Interestingly, it is not a directive but a regulation and is therefore - unlike the former - directly applicable. After the experiences of recent years, the European Union no longer had much confidence in its member states when it came to "adapting data protection standards".

In the aftermath, a shock wave went through the world of data protection. - Why was that?

Data protection activists in Germany were horrified because they feared that the data protection standards already in force in Germany would be lowered considerably. In contrast, other member states felt that the regulation would raise data protection to an absurdly high level. In fact, some Member States of the European Union wanted to reduce data protection to a minimum in order to gain national advantages. In this

context, the following question: In which Member State do most international IT groups have their European headquarters? Do you have an idea? In the Republic of Ireland! It is precisely Member States like this that are said to have been at issue at the time. It is not without reason that the General Data Protection Regulation also stipulates the so-called market place principle - a reaction to a chain of active data protection violations by such groups.

7. European Data Protection — an Export Hit and a Global Trend

Seven years after it came into force, the General Data Protection Regulation continues to pose considerable challenges for European economies. After all, personal data is also an economic asset! Nevertheless, many describe the regulation as an export hit and the so-called gold standard in data protection. Europe plays a pioneering role when it comes to data protection.

It is therefore understandable that many third countries are enacting new data protection laws based on the central principles of the General Data Protection Regulation, such as the Brazilian, Japanese, South Korean and also the Georgian data protection laws. Adaptation is also important for many countries because it enables them to obtain the European Commission's so-called adequacy decision - a decision on the comparability of the level of data protection - which is required for data transfers. Remember Article 45 of the General Data Protection Regulation.

8. Final Considerations

That was a par force ride through the history of data protection. It is true that its modern concept has only developed in recent decades. However, data protection is a good 2000 years old, as I hope I have been able to convey to you here. Its history is one that runs right through churches, wars and state abuse of power.

The journey is not over, it will continue! Data protection issues will increasingly play an important role. Data processing is advancing with seven-mile boots. What the confessing said in his confession in the Middle Ages could perhaps be overheard or passed on verbally by the confessor, the clergyman, but it could not be stored permanently and disseminated en masse. Things are different in today's digital world.

As annoying and bureaucratic as data protection can sometimes be - it is a truly "maltreated" right - it is ultimately indispensable. The proverbial "right to privacy solitude", meaning the „right to be left alone“, must continue to be guaranteed in the future.

Norbert Bernsdorff*

The "State of Play" of Data Protection in Georgia – 2024 Communication on EU Enlargement Policy**

The article discusses the main findings of the EU Commission's recent staff-working document "Georgia 2024 Report", which assesses the country's progress since December 2023, when the European Council granted Georgia candidate status. The paper aims to contemplate the main findings and assessments concluded in the Report regarding Georgia's progress in aligning the data protection legal framework with the EU acquis. Furthermore, the paper suggests a legal analysis of the EU Commission's conclusions on Georgia's legal compliance with the Council of Europe's legal instruments on data protection. Lastly, a specific chapter is dedicated to discussing the Georgian data protection authority's effectiveness in ensuring the protection of personal data and its supervisory role.

Keywords: *Georgian Personal Data Protection Law, progress report, EU acquis, Personal Data Protection Service of Georgia, legal compliance*.

1. Starting Point: "Georgia 2024 Report"

In October 2024, the European Commission (EU Commission) presented its staff-working document "Georgia 2024 Report"[1] . The "Georgia 2024 Report" accompanies the EU Commission's "2024 Communication on EU enlargement policy" to the European Parliament, the Council, the European Economic and Social Committee, and

* Doctor of Law, Professor at the Philipps University of Marburg; Retired Judge of the German Federal Court of Social Affairs; Former Data Protection Commissioner of the Lower Saxony Judiciary. The Author is a Member of the Editorial Board of the „Journal of Personal Data Protection Law".

** The publication represents a statement submitted in the scope of cooperation with the Georgian Personal Data Protection Service. It is dedicated to the issues of Georgia`s integration with the European Union.

[1] Brussels, 30 October 2024, SWD (2024) 697 final.

the Committee of the Regions. The report covers the period from 15 June 2023 to 1 September 2024. In its "Main Findings" on page 7, the EU Commission takes the view that its recommendations from 2023 were not implemented and remain valid. For 2025, it recommends that Georgia "aligns the data protection legal framework with the EU acquis: Regulation (EU) 2016/679 and Directive (EU) 2016/680." Under the heading "Chapter 23: Judiciary and Fundamental Rights," on page 41 of its report, the EU Commission states that, despite the adoption of its new Law on the Protection of Personal Data, the protection of personal data in Georgia is not fully aligned with the relevant EU secondary legislation[2] and that Georgia has still not signed the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, as modernised[3] . The EU Commission certifies that the Personal Data Protection Service (PDPS) does a "generally satisfactory job of monitoring the lawfulness of data processing and activities carried out at the central database for electronic communication identification data"; however, the PDPS must play a more active role, particularly in monitoring covert investigations. The EU Commission refers to statistical data for 2022 and 2023 provided by the PDPS itself.

Under the heading "Chapter 10: Digital Transformation and Media," the EU Commission complains on page 73 of its report that Georgia has only partially aligned its national law in the field of digital services with Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public-sector information[4] . It also makes the same accusation regarding other, more recent, secondary EU legislation.[5] In preparing its "Georgia 2024 Report," the EU Commission is using a "new method" developed for the conduct of accession negotiations in February 2020. This method involves grouping individual negotiation chapters into thematic clusters. In this context, compliance with the requirements of negotiation chapter 23, "Judiciary and Fundamental Rights," is being monitored particularly closely.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the Directive 95/46/EC ("General Data Protection Regulation"), OJ L 119, 4 May 2016, pp. 1 et seq.; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4 May 2016, pp. 89 et seq.

[3] Basic document: European Treaty Series – No. 108.

[4] OJ L 172, 26 June 2019, pp. 56 et seq.

[5] General Data Protection Regulation, OJ L 119, 4 May 2016, pp. 1 et seq.; Regulation (EU) of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC ("Digital Services Act"), OJ L 277, 27 October 2022, pp. 1 et seq.; Regulation (EU) of the European Parliament and of the Council of September 14, 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 ("Digital Markets Act"), OJ L 265, 12 October 2022, pp. 1 et seq.

2. The Dilemma of Blanket and Unfounded Legal Criticism

In its "Georgia 2024 Report," the EU Commission regularly fails to provide concrete evidence for its conclusions, including in its assessment of the "state of play" of data protection in Georgia. Instead, it provides the following general reference in footnote 2 on page 4:

"It (this report) is based on inputs from a variety of sources, including contributions from Georgia, EU Member States, European Parliament Reports and information from various international and non-governmental organisations. It also includes the results of comparative assessments and indices produced by other stakeholders, in particular in the area of the rule of law."

Of course, there are technical limitations to providing concrete evidence for a report on the state of play of reforms in more than 30 negotiation chapters or six clusters. Nevertheless, blanket and unfounded legal criticism without concrete examples or evidence is difficult to understand and leaves no room for improvement for the institutions being criticised.

One of the basic requirements of objective legal criticism is that it must clearly state the premises on which the criticism is based. It must be verifiably justified and include both positive and negative aspects. The basic function of legal criticism is the methodical identification of shortcomings, errors, and contradictions with the aim of improving practical procedures or conditions. Blanket and unfounded criticism of the law poses several problems. Above all, it can lead to a decline in cooperation because it is not constructive and does not offer any suggestions for improvement. It can also undermine trust in the criticising institution—in this case, the EU Commission—and create a negative atmosphere. Blanket criticism can "obscure" actual problems instead of solving them. Constructive criticism of the law can be recognised by the following characteristics: It cites specific evidence for the behavior being criticised and offers constructive suggestions for change. It is aimed at improving the situation. In terms of form, it must be expressed in a respectful and appreciative manner.

Unfortunately, the „Georgia 2024 Report“ on pages 41 and 73 does not meet the criteria for such a positive approach – including in terms of atmosphere – to Georgian data protection law and the PDPS, the institution that administers it, for the following reasons.

3. The Modernised Council of Europe Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data

Convention No. 108 in its original version was opened for signature on 28 January 1981, and was the first legally binding international treaty to establish principles of

data protection. In 2001, it was supplemented by an additional protocol. A modernised version of Convention No. 108 has now been available for ratification for some time. This "Convention No. 108+" will enter into force when 38 member states of the Council of Europe have ratified it.

It is understandable that the EU Commission calls on Georgia in its report to sign (and subsequently ratify) the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data in its modernised version. With Georgia's ratification of Convention No. 108+, its entry into force is finally one-step closer.

However, the European Court of Human Rights (ECtHR) – with its rulings -has long since assumed the role of a central decision-making authority on data protection issues for the member states of the Council of Europe. It does use Convention No. 108 as an interpretative aid. However, since 1987, it has derived the right to protection of personal data independently and decisively from the human rights enshrined in the European Convention on Human Rights (ECHR), in particular from Article 8 ECHR ("Right to Respect for Private and Family Life, Home and Correspondence"). Because the ECtHR does not rule directly on the basis of Convention No. 108, but on the basis of the human rights of the ECHR, the legal significance of Convention No. 108 "takes a back seat." Furthermore, this international treaty still only lays down general principles for the protection of personal data, such as the need for a legal basis for processing, transparency of processing, the right to information and rectification, and the establishment of control mechanisms.

Since the *Leander versus Sweden* judgement of 1987[6], in which the ECtHR analysed, for the first time, the question of the storage by a public authority of an individual`s personal data, the case-law in this field has seen significant development. Over the years the Court has examined many situations in which questions related to this issue have been raised. A broad spectrum of operations involving personal data, such as the collection, storage, use and dissemination of such data, is now covered by a body of case-law of the ECtHR. This case-law has developed in line with the rapid evolution in information and communication technologies.

The right to the protection of personal data is not an autonomous right among the various ECHR rights and freedoms. The Court has nevertheless acknowledged that the protection of personal data is of fundamental importance to a person`s enjoyment of his or her right to respect for private and family life, home and correspondence, as guaranteed by Article 8 of the ECHR[7]. This Article is the main vector through which personal data is protected in the ECHR system, even though considerations related to this protection may also come into play under other provisions of the ECHR and its Protocols.

[6] ECtHR, Case of Leander v. Sweden, Application no. 9248/81, hudoc.

[7] ECtHR, Case of Z v. Finland, Application no. 22009/93, hudoc; Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application no. 931/13, hudoc; Case of L.B. v. Hungary, Application no. 36345/16, hudoc.

As a result, Georgia is already unable to evade the legal standards established by the Council of Europe for data protection. Regardless of whether it signs (and subsequently ratifies) Convention No. 108+, Georgia is already bound by the established data protection case law of the ECtHR, meaning that "adoption" of Convention No. 108+ would, at most, be of a supplementary nature.

4. Alignment with the General Data Protection Regulation, the Digital Services Act, and the Digital Markets Act

In its "Georgia 2024 Report" on page 73, the EU Commission does not explain why it believes that the three legal texts mentioned, all of which are EU regulations ("Regulation," "Acts"), required Georgia to align its data protection law in advance of accession. From a legal perspective, EU directives are limited to prescribing a specific result to EU member states. They leave it up to the member states themselves to achieve this result; the member states must implement directives within certain time limits through their own national legislation. In contrast, EU regulations are directly and immediately binding on all EU member states and not, like a directive, only with regard to the result to be achieved. EU regulations do not, in principle, need to be transposed into national law.

The adoption of EU law upon accession to the EU – known as "adoption" or "transition" – is an automatic process.[8] The technical instrument for this is the "accession" of the candidate country. This takes place through the (international) accession agreement with all other EU member states. From the date of accession, the candidate country becomes a party to all EU treaties in their current version. All EU legislation adopted on the basis of these treaties up to the date of accession automatically becomes binding on the acceding state. It takes precedence over any national law. For EU data protection law, this means that it also automatically becomes part of the national legal system as primary law upon accession. It „grows“ into the national legal order.

Against this background, the EU Commission has failed to explain why, unlike existing EU Member States, the candidate country Georgia is required to "substitute" the content of the aforementioned EU regulations in its national data protection law prior to accession, i.e., to "anticipate" the EU regulations even before accession. If EU regulations also require the establishment of a minimum level of "enabling environment" in national law, corresponding clarifications and an outline of this "enabling environment" would have been desirable.

However, even if there were a need for the Digital Services Act to be "substituted" in Georgia's national data protection law, or at least to a greater extent, it would not be clear, without knowledge of the results of the TAIEX workshop in June

[8] See *Norbert Bernsdorff,* "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, N2, 2023, pp. 13 et seq.

2024, where and in what respects further alignments would have had to be made by September 2024:

The EU's Digital Services Act creates a single set of rules for online services to promote a safe digital environment and protect consumers.[9] Key points include stronger obligations for online platforms such as social networks and marketplaces to moderate content and deal with user complaints. The Digital Services Act calls for greater transparency regarding moderation processes and advertising, contains measures against hate speech and disinformation, and strengthens the protection of minors. Stricter rules apply to very large platforms.

In view of the extensive provisions of the Law of Georgia on Personal Data Protection regarding its scope (Article 2), it is not clear why the Law does not also require online intermediaries such as online platforms, social networks, marketplaces, and app stores to take responsibility for illegal content. It also needs to be explained why the complaint mechanisms set out in Chapter III of the Law ("Rights of Data Subjects") are not sufficient to take legal action against decisions made by platform operators. Finally, the Law of Georgia on Personal Data Protection contains numerous provisions on the obligations of controllers and processors (Article 23 et seq.). Under the PDPS, a national supervisory authority monitors compliance with data protection law, including by digital service providers (Article 49 et seq.).

The Digital Markets Act is an EU regulation that aims to promote competition in digital markets by regulating large online platforms with a dominant market position, known as so-called gatekeepers. The aim is to create fair conditions and prevent the abuse of market power. The Digital Markets Act prohibits certain behaviors by so-called gatekeepers, such as favoring their own services or hindering data transfer, and instead prescribes greater interoperability and fair conditions.

It is not obvious, nor does the EU Commission explain, why the "Do‘s" and "Don'ts" imposed on so-called gatekeepers in the Digital Markets Act in the interest of fair competition cannot already be enforced using the conventional instruments of Georgian data protection law (Article 13 et seq., Article 18, Article 64, Chapter X). Restricting consumers' use of third-party digital services may also be prohibited under Georgian data protection law, and so-called gatekeepers may be required to uninstall certain computer applications or software in the event of a conflict.

As far as the General Data Protection Regulation is concerned, the provisions of the Law of Georgia on Personal Data Protection already come very close to its requirements.[10] The law incorporates many principles from the General Data Protection Regulation, including data subject rights, transparency, security obligations, and data breach notifications.

[9] For further information: *Bernsdorff N.,* E-Commerce and Data Protection – The Digital Services Act and its National Implementation, Journal of Personal Data Protection Law, N2, 2024, pp. 7 et seq.

[10] See *Bernsdorff N.,* The New Data Protection Law – A Brief Outline, Journal of Personal Data Protection Law, N1, 2024, pp. 101 et seq.

5. Effective Supervision by the Personal Data Protection Service

Data protection authorities generally have to answer questions from all areas of data protection across all industries and as part of so-called cross-sectional audits. Where they can place trust in the controllers and processors of personal data, less supervision is needed, while in other areas, focused audits must be carried out on a regular basis. There is always a great need for advice and education in this area. When auditing data protection compliance, not all questions are always equally relevant. There are no "off-the-shelf" data protection solutions; measures applied by data protection authorities must correspond to the specific data protection risk identified. An impact assessment must also be carried out before such measures are taken. Against this background, it is almost impossible to assess whether data protection authorities – and thus the Georgian PDPS – are actively managing data and pursuing an effective data protection concept.

It is certainly not convincing to use staggered "case numbers" after several years (2022, 2023) to measure activity (and take as a basis for future forecasts), as the EU Commission has done in the graphic attached to its "Georgia 2024 Report" on page 41. This graphic shows a linear increase in all areas. With regard to the PDPS „Special Report“ on the activities for the first six months of 2025[11] , the EU Commission's suggestion that the PDPS should play a "more active role" here does not seem justified. In the first half of 2025, the number of inspections/examinations was 155. According to its statistics, the PDPS had received 496 applications/notifications. The Service identified 278 administrative offenses and imposed administrative sanctions in 277 cases. 369 instructions and recommendations were issued. The international activities of the PDPS, which it reported on in another "Special Report"[12] , are also worth highlighting. In view of the numerous checks described in the "Special Report" on the activities of the PDPS for the first six months of 2025 in the field of monitoring covert investigative actions[13] , which the PDPS is obliged to carry out under Chapter VII of the Law of Georgia on Personal Data Protection, it is not clear why, in the opinion of the EU Commission, there is still a need for increased action in this area.

[11] Statistics of the Activities of the Personal Data Protection Service of Georgia for 6 Months of 2025/January-June.
[12] International Activities carried out by the Service in 2022-2024 to implement the Best European Practices and Standards of Personal Data Protection Law.
[13] Pages 8 to 11.

Bibliography:

1. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) European Treaty Series No 108 (1981).
2. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the Directive 95/46/EC ("General Data Protection Regulation").
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.
5. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.
6. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
7. *Bernsdorff N.,* "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, N2, 2023, pp. 13 et seq.
8. *Bernsdorff N.,* E-Commerce and Data Protection – The Digital Services Act and its National Implementation, Journal of Personal Data Protection Law, N2, 2024, pp. 7 et seq.
9. *Bernsdorff N.,* the New Data Protection Law – A Brief Outline, Journal of Personal Data Protection Law, N1, 2024, pp. 101 et seq.
10. Case of L.B. v. Hungary, Application no. 36345/16, hudoc.
11. *European Commission***,** Staff Working Document SWD (2024) *697 final* (Brussels, 30 October 2024).
12. International Activities carried out by the Service in 2022-2024 to implement the Best European Practices and Standards of Personal Data Protection Law.
13. OJ L 172, 26 June 2019, pp. 56 et seq.
14. OJ L 119, 4 May 2016, pp. 1 et seq.
15. Statistics of the Activities of the Personal Data Protection Service of Georgia for 6 Months of 2025/January-June, Personal Data Protection Service of Georgia.

16. Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application no. 931/13, hudoc.
17. ECtHR, Case of Leander v. Sweden, Application no. 9248/81, hudoc.
18. ECtHR, Case of Z v. Finland, Application no. 22009/93, hudoc.

Maxime Gennart*

Privacy, Ethics and Collaboration: the Roles of DPAs in AI development**

First of all, I would like to thank the personal data protection service of Georgia for this very interesting three days and the warm welcome in Batumi. I also would like to thank them for giving me the opportunity of presenting with such a distinguished panel of speakers on the topic of Privacy, Ethics, and Collaboration: the roles of DPAs in AI development.

For those of you whom I have not had the honor to meet, my name is Maxime Gennart, I am a legal advisor at the Belgian data protection authority and a member of its AI task force. In this role, I am involved in setting up the Belgian national framework for AI governance, and it is on this topic I wanted to talk to you today.

Keywords: *Privacy, Ethics, Data Protection Authorities, AI, Privacy-by-Design, Ethics-by-design.*

1. Introduction

This article explores how Data Protection Authorities (DPAs) can guide the development of AI in a way that respects both privacy and broader human rights. To do so, it first illustrates the type of interdisciplinary thinking that AI development will require, using a real-world use case. It then explains how the concept of privacy-by-design provides a valuable tool for the responsible development of technologies and why its expansion into a broader notion of ethics-by-design should be considered. Building on this, the article highlights how DPAs' experience in implementing privacy-by-design is crucial for advancing a framework such as ethics-by-design. Finally, it examines how certain provisions of the AI Act could foster private–public cooperation in the development of AI, thereby supporting the case for collaborative pre-market value assignments.

* Legal Advisor at the Belgian Data Protection Authority.

** The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

2. Interdisciplinary Thinking & Cross-Sectoral Issues of AI

To exemplify the type of interdisciplinary thinking behind AI systems and the cross-sectoral issues they pose, I decided to talk briefly about Amazon's AI recruiting tool from 2018.

That experimental AI recruiting tool used a five-star rating system to score the likelihood of individuals getting software and technical job roles at Amazon.

It was trained for years using extensive datasets containing job applications, CV, cover letter, etc… The goal of the AI tool was to select the best candidates for technical and software jobs at Amazon.

To attain that goal, the tool spotted similarities across participant and sorted out the best ones. Now, it is a well-known fact that men are over-represented in software and technical jobs and the AI system was trained based on that fact.

Because of this, the tool began to skew reasoning towards this preference and quickly started showing signs of sexism, by lowering scores for resumes from women and steering preferences towards male candidates. In the end, and partly because of this discriminatory patterns, Amazon pulled this AI tool back.

Based on this example, we can already see how AI will affect a number of sectors and require the involvement of various disciplines. In this case, we can already see issues related to labor law, privacy & data protection, discrimination law, and the involvement of technical experts to adapt the tool and correct such biases.

3. Privacy-by-Design: The Collective Responsibility of Fundamental Rights

This example also shows that AI systems will affect individuals' life by having an impact on broader societal values that have to be implemented by technical experts.

This is not the first time we are seeing issues like this. We observed a similar fact with the rise of predictive technologies a few years ago. In fact, in the years following the Snowden revelations, the public started to become aware of the ways their personal data were being used online and how their fundamental right to data protection was being affected through the design of technologies.

This public awareness led to the realization that privacy and data protection could not solely rely anymore on individuals' decisions over their personal data. This led to a shift in the mind of people that personal data protection, although about individuals, became a collective responsibility that needed to be thought about holistically and implemented by technical profiles at the design phase. In addition, here came the concept privacy-by-design.

This shift was critical. It expressed the idea that compliance to common values, such as privacy and data protection, could be achieved or promoted at the design phase of a product more effectively than on an ex post basis through enforcement and corrective measures.

The rationale for privacy-by-design is thus both practical and philosophical. It rests on the understanding that the architecture of information systems can act as a form of regulation in itself.

4. Ethics-by-design: Embedding Universal Values at the Start

Today, this rationale remains entirely relevant. As exemplified with Amazon's AI recruiting tool, AI systems pose challenges to fundamental values that needs to be tackled across sectors.

However, privacy-by-design, as its name indicates, is about the safeguard of privacy, one fundamental rights among so many others. Privacy-by-design is thus in itself not sufficient anymore. That is where ethics-by-design could come in.

Ethics-by-design is about assigning values into the AI system's design that would guide it throughout its decision-making processes.

Given the breath of these challenges and the number of fundamental rights potentially affected, it may seem only logical to try and attribute significance or even moral worth to the decisions taken by AI systems.

While this is relatively easy on paper, how to technically instruct an AI system to reach the goal of presenting the best applicant while keeping in mind that this shouldn't be carried out based on gender is a complex and intricate task that would require the input of individuals from various backgrounds.

Practically, this shift would require us to shift from a reactive type of regulation to a more proactive one. Such as privacy-by-design require us to think about privacy when deciding the means and the way of a processing operation, ethics-by-design would require us to think about the values that will serve as guiding line for AI systems' decisions.

5. DPA's Experience to the Rescue

How can DPAs' experience implementing the concept of privacy-by-design be of help with the development and implementation of the ethics-by-design concept?

Well, as data protection authorities, we have a wealth of experience conducting complex balancing exercises. We assess the necessity and proportionality of processing operations in a wide range of contexts by weighing data protection rights against freedom of expression, freedom of information, public interest, and more.

The balancing exercises that we carry out often requires us to combine interdisciplinary knowledge. We ask for the input of technical experts to fully comprehend the implications of a specific processing operation. We then come with our own legal expertise to identify the obligations applicable to the processing at hand. Thanks to this cooperation, we understand whether privacy was truly thought of at

the design phase of the processing operation or as an afterthought following an investigation or a complaint.

These skills makes us uniquely positioned to:

- Identify risks posed by AI systems,
- Think rationally and ethically in balancing rights, values and interests at stake, and
- Find a legitimate compromise between conflicting values.

In the regulation of AI systems and the potential shift from privacy by design to ethics-by-design, we, DPAs, therefore have a necessary experience to gather people with relevant knowledge to understand the intricacies of a specific technological environment and try to implement/assign a value that would guide AI systems throughout their lifecycle.

Now, how could we practically start to enable such a shift and how could that shift look like?

To answer that question, I will elaborate on five situations where we can see the shift appearing. Three are post-market monitoring practices, two others happen before entering the market.

6. From Post-Market Cooperation Mechanism

First, I believe the FRIA[1] is a first ex-ante assessment of high-risk AI Systems and is invaluable. It prompts designers to evaluate ethical trade-offs early in the design phase, not as an afterthought. There is therefore an opportunity to include an ethics-by-design thinking into AI development. The issue, if I may, is similar to DPIA, is that it is entirely carried out by private actors developing the assessed technology.

Second, we can look at the work carried out by international organization such as the EU, the OECD, UNESCO, etc. These initiatives are a great example of cooperation because they usually include the input of both the private and the public sector to work towards the translation of fundamental rights into values that AI systems could be asked to consider. However, these standards are not enforceable and their implementation is entirely left to the discretion of private actors.

You can already see here that the point I am trying to make is that there is still this huge gap between the private actors, technical experts and designers of technologies, and public authorities, experts in enforcing and implementing fundamental rights. In addition, here comes the AI Act.

Its article 79(2) already starts to close this gap. According to this article, Market surveillance authorities (MSA) which identify a risk to fundamental right(s), have to notify the relevant authority protecting that fundamental right. Together with the operator of the concerned AI system, they have to cooperate in remediating that risk.

[1] Disclaimer: the FRIA is here included under the post-market monitoring because it is written from a Litigation perspective. I am aware that this is an internal ex ante assessment carried out by private actors. However, as DPAs, they only appear when a complaint has been filed.

In this scenario, there is an obligation of cooperation between the private sector, MSA and DPAs to adapt the design of an AI system and ensure it respects the fundamental right to privacy and data protection. However, here we can say that the intervention arrives a bit late, as a risk has been identified and will potentially have materialized.

However, given the characteristics of AI systems and the real-world implications they already have, such cooperation mechanism involving ethical tradeoffs and value assignment exercises should be fostered to take place at the design phase and with the involvement of both the developer of the AI system and the authorities protecting fundamental rights.

To show you that this pre-market value assignment cooperation mechanism is feasible in practice, I wanted to draw your attention on two provisions of the AI Act.

7. To Pre-Market Value Assignment Cooperation

The first disposition relates to the regulatory sandboxes of art. 57 AIA. The article explains that member states should have at least one regulatory sandbox. The aim of these sandboxes is to identify possible risks, in particular to fundamental rights. A derived aim of these sandboxes is to promote innovation that adhere and respects fundamental rights, including the one to data protection.

Now what is also interesting is that, in its paragraph 4, it opens up the possibility for the authority responsible to operate the national regulatory sandbox to cooperate with other authorities in testing the AI system. From this disposition, we thus have an opening to operate some kind of pre-market monitoring of high-risk AI systems. Indeed, we, as public authorities protecting fundamental rights, could be asked to participate in the testing of high-risk AI systems. This would pave the way towards a cooperation between public and private actors involved in the testing of an AI system to adapt or modify it for it to respect fundamental rights, before its placing on the market.

Besides testing in controlled environment like regulatory sandboxes, the AI Act also offers the possibility to test high-risk AI systems in real-world conditions outside of regulatory sandboxes. This, of course has to be done, under a number of strict conditions among which the submission of a testing plan by the AI system operator to the national competent authority and the transmission of the final outcome of that real-world test to that same authority.

If that competent authority finds it necessary, it can monitor that testing by, among other, carry out onsite or remote inspection during the testing.

The national competent authority therefore has the possibility to either analyses the AI system live when it is being tested or analyses it after the test based on the final outcome transmitted by the operator.

Now, imagine that authority identifies a risk to the fundamental right to data protection, wouldn’t that trigger the notification and remediation mechanism of art. 79(2)? Hence, wouldn’t that trigger another type of pre-market cooperation

mechanism involving authorities protecting fundamental rights, market surveillance authorities and private actors?

The opportunities indeed seems to be present.

8. Conclusion

I would like to conclude by saying that although the challenges and risks posed by AI are numerous, similar concerned were raised with the rise of predictive technologies at a time where data protection was being strengthened.

The experience we, as DPA, have acquired in addressing intricate questions about fundamental values in complex technological environment is crucial to start thinking about the development of a pre-market ethics-by-design approaches to AI development and innovation.

Agnieszka Grzelak*

Reconciling Data Minimization with Model Maximization: Regulatory and Ethical Tensions in AI Development**

The rapid advancement of large-scale artificial intelligence (AI) systems, particularly large language models (LLMs), has created profound regulatory tensions in the realm of data protection. Central to this discourse is the conflict between the principles of data minimization, as enshrined in the General Data Protection Regulation (GDPR), and the data-intensive logic underpinning AI model development. This article explores some aspects of the legal, practical, and ethical implications of this tension from the perspective of data protection authorities (DPAs), analyzing current enforcement trends, regulatory guidance, and the prospective impact of the EU Artificial Intelligence Act. It argues that DPAs must evolve beyond traditional enforcement roles to become ethical stewards and proactive coordinators of AI governance in Europe to ensure that the fundamental principles are not weakened or ignored in the name of innovation.

Keywords: *Data Minimization, AI Act, Large Language Models (LLMs), General Data Protection Regulation (GDPR), Ethical AI Governance.*

1. Introduction: Data Protection in the Age of Expansive AI Models

The increasing integration of artificial intelligence (AI) technologies into public services, private enterprise, and everyday life has intensified longstanding tensions between innovation and the protection of fundamental rights. Among the most acute

* Dr Habil of Legal Sciences, Professor at the Kozminski University in Warsaw (PhD 2000, The Jagiellonian University Cracow; Habil. 2016 Polish Academy of Science). Deputy President of the Personal Data Protection Office, Warsaw – Poland; a_grzelak@uodo.gov.pl. https://orcid.org/0000-0002-5867-8135

** The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

of these is the emerging conflict between the GDPR's foundational principle of data minimization and the data-intensive logic that drives the development of contemporary AI systems, especially large language models (LLMs).

The GDPR establishes data minimization as a bedrock principle of lawful data processing[1]. According to Article 5(1) (c), personal data must be "adequate, relevant and limited to what is necessary" in relation to the purposes for which it is processed. This mandate aims to curtail the collection and use of unnecessary personal data and to promote accountability, transparency, and respect for data subjects' rights. However, in the context of AI model development, particularly LLMs, this principle is increasingly under strain.

LLMs function on the premise of scale: the broader and more diverse the dataset, the more nuanced and powerful the model becomes[2]. Developers thus often rely on indiscriminate web scraping to collect vast data, including personal data, from across the public internet. The guiding assumption is that more data translates into better model accuracy, contextual awareness, and adaptability. Yet this assumption introduces a structural opposition to data minimization, as such models are built not to minimize data input, but to maximize informational capture and generalization capabilities.

Notably, most of the leading LLMs are developed by entities headquartered outside the European Union. This raises additional challenges regarding jurisdiction, enforcement, and the extraterritorial applicability of the GDPR. European users' personal data may be processed by non-EU actors who do not fully internalize the normative and legal obligations set forth by EU law. Consequently, European Data Protection Authorities (DPAs) face a growing imperative to assert the relevance of EU data protection principles in global technological contexts.

In response to these challenges, the European Data Protection Board (EDPB) has increasingly called for a more expansive interpretation of DPA responsibilities. In its Statement 3/2024, issued in July 2024, the EDPB clarified that DPAs are not merely reactive regulators, but also proactive advisors, coordinators, and ethical arbiters under the forthcoming AI Act[3]. This reconceptualization underscores the need for DPAs to engage not only in enforcement, but in strategic governance and anticipatory oversight of AI technologies.

The present article aims to explore the implications of this evolving regulatory landscape, with a particular focus on the tensions between data minimization and model maximization. It interrogates how DPAs can meaningfully safeguard data protection principles in an era where data volume, rather than data discipline, is increasingly seen as a marker of technological success. Through legal analysis,

[1] *Kuner C., Bygrave L. A., Docksey C.,* The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020.

[2] *Vaezi A.,* Legal Challenges in the Deployment of Large Language Models: A Comparative Analysis under the GDPR and EU AI Act, 2025.

[3] European Data Protection Board, Statement 3/2024 on the role of DPAs under the AI Act, 2024, <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en> [23.07.2025].

regulatory interpretation, and consideration of emerging enforcement practices, this study contributes to an urgent conversation about the future of responsible AI in the European Union and beyond.

2. Structural Incompatibilities between Data Minimization and AI Model Development

The rapid evolution of large-scale artificial intelligence systems has brought to the forefront a foundational question in contemporary data protection law: Are we witnessing an unavoidable conflict between legal principles and technological practice? At the core of this dilemma lies a fundamental tension between the GDPR's principle of data minimization and the operational architecture of modern machine learning models, particularly large language models (LLMs).

The GDPR, specifically Article 5(1) (c), establishes the principle of data minimization as a cornerstone of lawful data processing[4]. This principle requires that personal data collected must be adequate, relevant, and limited to what is strictly necessary for the specific purposes for which it is processed. In practice, this means that organizations must refrain from collecting or retaining data unless it can be clearly justified in terms of purpose and necessity.

In stark contrast, the logic underlying LLM development is premised on data abundance. The prevailing assumption among AI developers is that the performance and generalizability of these models improve with the volume and diversity of training data. Consequently, LLMs are typically trained on massive datasets encompassing billions of text samples—ranging from academic publications to forum posts, blogs, social media content, and other publicly accessible sources. The aspirational goal is comprehensive linguistic coverage and semantic richness, but this data-centric philosophy directly challenges the necessity and proportionality constraints imposed by the GDPR.

This structural conflict manifests in several critical ways. First, the practice of indiscriminate web scraping often lacks a narrowly defined purpose compatible with data minimization. The mere assumption that all accessible textual data may contribute to model improvement is insufficient under EU data protection law, which requires specific and legitimate processing aims. Furthermore, the scale of collection typically far exceeds what would be considered necessary for the stated objectives of the model, particularly when personal data is involved.

The European Data Protection Board (EDPB), in its Opinion 28/2024, has underscored the importance of rigorous necessity assessments. The Board maintains that personal data embedded within training datasets—even when not directly

[4] *Kuner C., Bygrave L. A., Docksey C.,* The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020.

identifiable—may give rise to re-identification risks[5]. Deep learning models, by virtue of their architecture, can memorize and reproduce training data verbatim or in paraphrased form. This introduces a latent threat that personal information, once included in the training corpus, may later be exposed through model outputs, even in the absence of deliberate intent by the developer.

The EDPB has also drawn attention to the inadequacy of generic anonymization claims. Assertions that personal data has been sufficiently de-identified or pseudonymized must be substantiated by model-specific evaluations and cannot rely on abstract technical assumptions. Inference attacks, model inversion, and membership inference techniques have demonstrated that anonymized data may, under certain conditions, be reverse-engineered or linked back to individuals. These risks necessitate a cautious, case-by-case analysis of the technical safeguards employed in model training.

Moreover, the principle of proportionality is central to the legality of data processing. Controllers must establish a defensible relationship between the quantity of personal data processed and the benefit sought through AI system performance. In the case of LLMs, however, the boundaries of necessity and proportionality are often blurred. Developers frequently fail to articulate why a specific dataset size or composition is required, or why more targeted and privacy-preserving alternatives were not pursued.

The conflict is therefore not merely theoretical but deeply practical. AI developers operate within a paradigm that rewards maximal data ingestion, while data protection frameworks demand restraint, justification, and user-centric safeguards. Bridging this gap will require not only regulatory clarity and enforcement, but also a paradigm shift in how AI innovation is conceptualized.

To move toward compatibility, AI development must increasingly integrate the principles of privacy by design and privacy by default, as mandated under Article 25 of the GDPR. This entails embedding data minimization logic into the architecture of AI systems from their inception. It also implies adopting methodologies that reduce dependency on personal data—such as synthetic data generation, federated learning, or differential privacy mechanisms—thereby aligning technological advancement with legal obligations.

In conclusion, the perceived dichotomy between data minimization and model maximization is emblematic of broader governance challenges in the digital age. While not inherently irreconcilable, these opposing logics require deliberate reconciliation through multidisciplinary collaboration, technical innovation, and regulatory vigilance. Without this effort, the integrity of fundamental rights may be undermined by the unchecked pursuit of technological optimization.

[5] European Data Protection Board, Opinion 28/2024 on Training Data for LLMs, 2024, <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en> [23.07.2025].

3. Publicly Accessible Data and the Legal Status of Personal Information under the GDPR

A pervasive assumption among AI developers may be that publicly available data is inherently exempt from the full scope of data protection regulation. This misconception underpins many arguments defending the collection and use of large-scale datasets for training AI models, including large language models (LLMs). Developers often argue that because the data used is already accessible on the open web, it does not fall within the regulatory protections of the General Data Protection Regulation (GDPR)[6]. However, such reasoning is legally and ethically flawed.

Under the GDPR, the status of data as "personal" is determined by its identifiability, not its availability. Article 4(1) of the GDPR clearly defines personal data as any information relating to an identified or identifiable natural person, regardless of whether that information was obtained from private or public sources. Thus, the fact that personal data appears on public forums, social media, comment sections, or other open-access domains does not strip it of its protected status.

This legal position has profound implications for the development of AI systems, particularly those trained on data scraped indiscriminately from the internet. The European Data Protection Board (EDPB) has expressed concern about this issue in several recent opinions, most notably in Opinion 28/2024. The EDPB emphasizes that the legality of using such data for training AI models must be assessed on a case-by-case basis. A key point is that the process of data anonymization—often cited by developers as a compliance measure—cannot be presumed effective without rigorous, model-specific validation.

Even if an AI model is not designed to output personal data directly, there remains a significant risk that personal information embedded in the training corpus may be retained within the model's parameters. This latent data may be unintentionally reconstructed in response to user prompts, thereby creating the potential for privacy violations through inference or re-identification. Recent academic studies and real-world incidents have demonstrated that LLMs can inadvertently reproduce specific personal details, such as names, addresses, or fragments of private conversations, raising serious questions about the sufficiency of standard anonymization techniques in the AI context.

In light of these risks, DPAs are increasingly scrutinizing claims of anonymization and demanding transparency about training data composition. To properly assess compliance, regulators must have access to detailed technical documentation, including dataset sources, preprocessing methods, and mitigation strategies. This reinforces the need for regulatory bodies to invest in technical expertise and cross-disciplinary capacity building. Without such capabilities, DPAs cannot perform the

[6] Opinions presented during meeting with Polish DPA. Cf. <uodo.gov.pl> for more information on the meetings with OpenAI or Microsoft.

granular assessments necessary to evaluate whether data minimization, necessity, and proportionality standards have been met.

Furthermore, the principle of privacy by design, articulated in Article 25 of the GDPR, requires that data protection safeguards be embedded into processing activities from the outset. This entails conducting thorough data protection impact assessments (DPIAs) before the commencement of training operations, with a clear articulation of the purpose, scope, and limitations of data collection. Developers must explicitly define what categories of personal data are essential to achieve a model's objectives and demonstrate that less invasive alternatives were considered.

Equally important is the concept of proportionality, which demands a demonstrable relationship between the quantity and sensitivity of personal data processed and the legitimate aims pursued. Massive and indiscriminate scraping of online content—especially without contextual filtering or consent—raises substantial doubts about proportionality and undermines user trust in digital ecosystems.

The idea that "public equals permissible" must be unequivocally rejected. The mere fact that information is accessible online does not confer a license to repurpose it for machine learning without appropriate legal and ethical safeguards. It is a duty of DPAs to challenge this norm and to reinforce the distinction between visibility and validity in data governance.

In conclusion, the lawful use of public data in AI development is far from a settled issue. It calls for robust legal interpretation, rigorous technical scrutiny, and a proactive regulatory posture to ensure that individual rights are not subordinated to the imperatives of technological expansion.

4. Legal Bases for Processing in AI Model Training: Consent, Legitimate Interests, and the Challenge of Transparency

Establishing a valid legal basis for the processing of personal data used in training AI models—particularly large language models (LLMs)—is one of the most complex and disputed issues in the current regulatory landscape. Despite the growing reliance on massive data corpora for developing AI capabilities, many developers have not clearly articulated how such processing complies with the General Data Protection Regulation (GDPR), especially in light of Articles 6, 7, 13, and 14.

While consent is often heralded as the gold standard for lawful processing under the GDPR, its practical application in the AI training context is fraught with difficulty. Article 4(11) defines consent as a freely given, specific, informed, and unambiguous indication of the data subject's wishes. However, this standard is rarely met when consent is sought through general terms of service, opaque privacy policies, or platform-level notices. When personal data is scraped from public websites or user-generated content platforms, there is typically no meaningful opportunity for data subjects to give or withhold consent—let alone understand how their data will be

repurposed in AI systems. As such, reliance on consent in these contexts is often legally insufficient and ethically dubious.

In practice, many developers turn to the legal basis of legitimate interest under Article 6(1)(f) as a more flexible alternative[7]. However, the threshold for invoking this basis is stringent. The controller must conduct a comprehensive three-part balancing test: (1) identify a legitimate interest pursued by the data controller or a third party, (2) demonstrate that the processing is necessary for achieving that interest, and (3) prove that the interest is not overridden by the rights and freedoms of the data subject. According to the EDPB's 2024 Guidelines on AI and data processing, this assessment must be both objective and evidence-based, and must be supported by documented safeguards, accountability measures, and mitigation strategies for data subject risk.

A central difficulty in this approach is that necessity and proportionality are rarely self-evident in the context of LLM development. Given the scale and opacity of data scraping, and the speculative nature of benefits derived from diverse training data, it is often unclear whether processing is strictly necessary for the stated purpose or merely convenient for maximizing model performance. The burden of proof lies with the controller to explain why alternative, less invasive methods could not achieve similar results.

Compounding these challenges is the obligation to ensure transparency under Articles 13 and 14 of the GDPR. These provisions require data controllers to inform data subjects about the collection and use of their personal data—whether obtained directly or indirectly. In the context of AI training based on large-scale scraping from multiple platforms, fulfilling this obligation becomes nearly impossible. Developers rarely have access to the identities or contact information of individuals whose data was included in training sets, and retroactive notification is operationally unfeasible.

Nevertheless, the GDPR does not offer an exception to transparency obligations on the basis of scale or technical impracticality. In the absence of effective transparency mechanisms, the lawfulness of the underlying data processing is undermined. This has profound implications for developers seeking to rely on legitimate interest: if affected individuals are not informed, their ability to exercise their rights—such as the right to object under Article 21—is compromised, further weakening the legitimacy of the processing activity.

Moreover, transparency is not only a legal requirement, but also a vital ethical and societal imperative. Trust in AI systems—and in the institutions that govern them—depends on the ability of individuals to understand how their data is being used, and to retain some measure of control over that use. The opacity of many LLMs,

[7] *Sangaraju V. V.,* AI and Data Privacy in Healthcare: Compliance with HIPAA, GDPR, and Emerging Regulations, International Journal of Emerging Trends in Computer Science and Information Technology, 2025, 67–74.

both in terms of their training data and their functioning, exacerbates a broader accountability gap that undermines democratic oversight and public confidence.

In conclusion, the legal bases most commonly invoked for AI training—consent and legitimate interest—are both highly problematic in practice[8]. Developers must go beyond superficial compliance and engage with the spirit of data protection law by embedding transparency, accountability, and necessity into the design and deployment of AI systems. Without such efforts, reliance on these legal grounds may not only fail to meet regulatory scrutiny, but also erode the legitimacy of AI development in the eyes of the public and policymakers alike.

5. Enforcement Trajectories and Strategic Regulatory Responses to AI Data Practices

The enforcement of GDPR provisions in the realm of AI development represents one of the most demanding areas of contemporary data protection. The complexity of AI systems, especially large language models (LLMs), presents regulators with multifaceted challenges, including technical opacity, globalized data flows, and cross-jurisdictional accountability gaps. Despite these barriers, there has been a notable evolution in the posture of European data protection authorities (DPAs), who are increasingly moving from reactive enforcement to coordinated and proactive oversight.

One of the most significant enforcement milestones occurred in 2023, when the Italian Garante per la protezione dei dati personali imposed a temporary ban on ChatGPT. The decision was based on multiple grounds, including the lack of a lawful basis for data processing, insufficient transparency, and the absence of mechanisms to enable data subjects to exercise their rights. This marked the first high-profile intervention by a European DPA against a foundation model, signaling that large-scale AI systems are not immune to GDPR enforcement[9].

Other DPAs have followed suit with both enforcement and guidance. France's CNIL has issued comprehensive recommendations on web scraping, emphasizing that public accessibility does not equate to legal permissibility[10]. The UK's Information Commissioner's Office (ICO) similarly published guidelines articulating the conditions under which AI developers can legally use publicly sourced data for training

[8] *Hoofnagle C. J., van der Sloot B., Zuiderveen Borgesius F.,* The European Union General Data Protection Regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 2019, 65–98.

[9] Garante per la protezione dei dati personali, Decision on OpenAI (ChatGPT), 2023, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9870832> [23.07.2025].

[10] CNIL, First Recommendations on the Development of AI Systems, Commission Nationale de l'Informatique et des Libertés, 2024, <https://www.cnil.fr/en/ai-cnil-publishes-its-first-recommendations-development-artificial-intelligence-systems> [23.07.2025].

purposes[11]. Meanwhile, Greece's Hellenic Data Protection Authority imposed a €20 million fine on Clearview AI, establishing a precedent for holding biometric data scrapers accountable under GDPR provisions[12]. These actions illustrate the increasing willingness of DPAs to challenge powerful AI actors.

A key development at the European level is the emergence of joint enforcement mechanisms. The European Data Protection Board (EDPB) has launched dedicated task forces—most notably those concerning ChatGPT and DeepSeek[13]—that enable coordinated investigations and harmonized interpretations across Member States. These efforts are likely to be institutionalized under the AI Act, which introduces an EU-wide AI governance framework featuring the European Artificial Intelligence Office and enhanced cross-border supervisory structures. These new arrangements echo the GDPR's "One-Stop-Shop" model but with a stronger emphasis on systemic risk assessments and sector-specific oversight.

In parallel, DPAs are beginning to articulate forward-looking regulatory strategies. These include issuing proactive guidelines, demanding algorithmic impact assessments, and exploring technical audit procedures for model explainability and training data lineage. The trajectory is clear: enforcement is no longer confined to penalizing past violations but now encompasses ex ante regulation designed to prevent systemic harms before they materialize.

6. Ethical Oversight in AI Development: Expanding the Role of Data Protection Authorities

While legal frameworks such as the GDPR and the upcoming AI Act provide formal criteria for compliance, they are not always equipped to fully address the ethical dimensions of AI development. The use of personal data to train generative AI models invokes broader societal concerns related to human dignity, individual autonomy, and cultural representation. Practices that are technically lawful under a narrow interpretation of the law may still provoke ethical unease, public backlash, or social harm.

One salient example is the use of expressive personal data—such as voice recordings, biometric images, or creative content—to generate synthetic media. While developers may argue that such uses fall within lawful grounds if the data was publicly accessible, this overlooks the deeper issue of consent, artistic ownership, and the right

[11] ICO, The Lawful Basis for Web Scraping to Train Generative AI Models, Information Commissioner's Office (UK), 2024, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/response-to-the-consultation-series-on-generative-ai/the-lawful-basis-for-web-scraping-to-train-generative-ai-models/> [23.07.2025].

[12] Info on: <https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en> [23.07.2025].

[13] *Deng Z., Ma W., Han Q. L., Zhou W., Zhu X.,* Exploring DeepSeek: A Survey on Advances, Applications, Challenges and Future Directions, IEEE/CAA Journal of Automatica Sinica, 12(5), 2025, 872–893.

to one's likeness. In creative and journalistic sectors, unauthorized use of archival material to train AI-generated voices or avatars has been widely condemned as exploitative. Such practices erode professional integrity and diminish the ability of individuals to control how their identities are digitally reproduced.

These concerns extend beyond individual harms to systemic risks, including deepfakes, disinformation, political manipulation, and cultural homogenization. Synthetic content generated by LLMs or multimodal AI systems can be used to imitate real individuals, skew public discourse, or undermine democratic processes. The ethical implications of such uses are profound and not always foreseeable at the point of data collection or model training.

Recognizing these risks, the EDPB has called upon DPAs to assume a broader ethical mandate. Beyond ensuring formal compliance, DPAs are increasingly expected to identify power asymmetries between individuals and developers, evaluate the societal impact of large-scale data exploitation, and promote responsible innovation. Ethical assessment should therefore be treated as a complementary dimension of data protection governance, integrated into risk-based regulation and transparency obligations.

To fulfill this role effectively, DPAs must develop interdisciplinary capacities—encompassing legal, technical, sociological, and philosophical expertise—and cultivate dialogue with affected communities, civil society organizations, and academic researchers. Ethical oversight should be embedded in algorithmic design through mechanisms such as fairness audits, participatory model evaluations, and public interest impact statements.

In sum, ethical stewardship is emerging as a critical extension of the regulatory function. It repositions DPAs not only as guardians of legality but as arbiters of justice in a rapidly evolving technological landscape. Only by aligning legal compliance with ethical legitimacy can the governance of AI systems uphold public trust and fundamental rights in the digital era.

7. Future Directions: Integrating the AI Act and Addressing Institutional Challenges

The – already mentioned - European Union Artificial Intelligence Act (AI Act) represents a landmark regulatory initiative that introduces a comprehensive, risk-based framework for governing AI systems. Building upon the foundations established by the GDPR, the AI Act imposes heightened obligations for so-called high-risk AI applications. These include, among others, mandatory conformity assessments, structured technical documentation, robust data governance frameworks, and post-market monitoring requirements.

One of the most significant contributions of the AI Act is the operationalization of data quality and data minimization principles within the AI lifecycle. Article 10 (3) of the AI Act explicitly mandates that datasets used for training, validation, and testing

must be "relevant, representative, free of errors, and as complete as possible," while also emphasizing that they should be minimized in scope to avoid unnecessary exposure of personal data. In this sense, the Act strengthens the normative trajectory initiated by the GDPR by embedding data protection standards directly into AI system design and evaluation.

For Data Protection Authorities (DPAs), the implementation of the AI Act signifies both an expansion of responsibilities and a transformation of institutional identity. DPAs will no longer act solely as national enforcers of data privacy but must evolve into key nodes in a pan-European network of AI governance. This includes collaboration with the newly established European Artificial Intelligence Office, participation in cross-border investigations, contribution to harmonized guidance, and oversight of high-risk AI systems deployed across multiple sectors, including health, education, employment, and law enforcement.

However, this transition is fraught with challenges. Many DPAs currently face substantial resource limitations, including understaffing, limited technical infrastructure, and insufficient in-house expertise in machine learning, algorithmic auditing, and systems engineering. The new responsibilities outlined in the AI Act—such as the capacity to evaluate training data lineage, assess algorithmic impact, and ensure conformity with design-level transparency—will require significant investment in organizational capacity, skills development, and institutional coordination.

Another source of complexity arises from the doctrinal and operational intersections between the GDPR and the AI Act. Developers must navigate overlapping, and at times potentially conflicting, obligations concerning data minimization, lawful basis for processing, fairness, accountability, and data subject rights. These overlaps will necessitate interpretative guidance from the EDPB and the European AI Office to ensure coherent and non-redundant enforcement. The development of joint compliance frameworks and model templates may help to bridge regulatory gaps and promote legal certainty for developers operating across multiple EU jurisdictions.

Finally, the global nature of AI development poses challenges to the enforcement reach of European regulations. Many foundational models are developed outside the EU, and their integration into local products or services often obscures jurisdictional boundaries. The success of the AI Act will depend on the ability of European regulators to assert extraterritorial influence through cooperation mechanisms, adequacy frameworks, and public procurement incentives that favor compliant systems.

In sum, the AI Act offers an unprecedented opportunity to align technological innovation with democratic values and fundamental rights. Yet its implementation will require robust institutions, cross-sectoral cooperation, and sustained political commitment to make responsible AI not just a regulatory aspiration, but an operational reality.

8. Conclusion: From Legal Compliance to Ethical and Strategic Stewardship

The principle of data minimization, once seen as a technical constraint or bureaucratic formality, has emerged as a normative bulwark against surveillance capitalism, algorithmic exploitation, and asymmetries of power in the digital era. In an age increasingly defined by model maximization and data commodification, it serves as both a legal requirement and a moral imperative.

Yet the application of this principle must evolve in response to the unique complexities posed by contemporary AI systems. Large language models and other foundation models challenge conventional legal categories and procedural safeguards, calling for a more dynamic and holistic approach to regulatory enforcement. As such, Data Protection Authorities must reconceptualize their mandate—not only enforcing compliance, but fostering systemic accountability, ethical reflection, and public trust.

This expanded role entails resisting unjustified or disproportionate data practices, promoting transparent and explainable AI, and safeguarding the rights and freedoms of individuals whose data underpins digital innovation. It also requires building institutional capacity to conduct risk-based audits, engage with civil society, and contribute to the ethical governance of AI technologies.

Ultimately, the responsible development and deployment of AI cannot be reduced to a checklist of legal obligations. It is a collective societal commitment to embedding human dignity, fairness, and justice at the core of technological progress. In this endeavor, DPAs are not just regulators—they are stewards of the digital public interest.

Bibliography:

1. CNIL, First Recommendations on the Development of AI Systems, Commission Nationale de l'Informatique et des Libertés, 2024, <https://www.cnil.fr/en/ai-cnil-publishes-its-first-recommendations-development-artificial-intelligence-systems> [23.07.2025].
2. *Deng Z., Ma W., Han Q. L., Zhou W., Zhu X.,* Exploring DeepSeek: A Survey on Advances, Applications, Challenges and Future Directions, IEEE/CAA Journal of Automatica Sinica, 12(5), 2025, 872–893.
3. European Data Protection Board, Statement 3/2024 on the role of DPAs under the AI Act, 2024, <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en> [23.07.2025].
4. European Data Protection Board, Opinion 28/2024 on Training Data for LLMs, 2024 <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en> [23.07.2025].
5. Garante per la protezione dei dati personali, Decision on OpenAI (ChatGPT), 2023, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9870832> [23.07.2025].
6. *Hoofnagle C. J., van der Sloot B., Zuiderveen Borgesius F.,* The European Union General Data Protection Regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 2019, 65–98.
7. ICO, The Lawful Basis for Web Scraping to Train Generative AI Models, Information Commissioner's Office (UK), 2024, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/response-to-the-consultation-series-on-generative-ai/the-lawful-basis-for-web-scraping-to-train-generative-ai-models/> [23.07.2025].
8. *Kuner C., Bygrave L. A., Docksey C.,* The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020.
9. *Sangaraju V. V.,* AI and Data Privacy in Healthcare: Compliance with HIPAA, GDPR, and Emerging Regulations, International Journal of Emerging Trends in Computer Science and Information Technology, 2025, 67–74.
10. *Vaezi A.,* Legal Challenges in the Deployment of Large Language Models: A Comparative Analysis under the GDPR and EU AI Act, 2025.

Koba Grialashvili*

Personal Data Protection in the Activities of Law Enforcement Bodies

Globalization has introduced new challenges in the field of personal data processing, significantly increasing its overall scale. In this context, it is particularly important to highlight the extensive processing of personal data by law enforcement bodies. In order to fulfil their legally assigned powers, these agencies are authorized to obtain data from both open and covert sources and to process it through various means. Technological advancements have further enabled law enforcement bodies to process personal data on an unprecedented scale.

This article will focus on data processing standards, taking into account the specific nature of law enforcement activities. Such processing requires maintaining an appropriate balance between the objectives of protecting public security interests and safeguarding the rights of data subjects.

This paper will examine Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, and on the free movement of such data (hereinafter referred to as the LED)[1].

The discussion will focus on several key components of the Directive, including its purpose, rationale for adoption, and the data processing principles it establishes. Particular attention will be given to the rights of data subjects — one of the fundamental pillars of personal data protection law — and to the international instruments adopted to ensure their protection and reinforcement.

Keywords: *LED, data subject rights, crime prevention, investigation, prosecution or execution of sentence, protection of public safety.*

* PhD candidate at the Faculty of Law, East European University; Head of the Secretariat of the Committee on Human Rights and Civil Integration, Parliament of Georgia.

[1] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (hereinafter referred to as the LED).

1. Introduction

The European Union is widely regarded as a global leader in the field of personal data protection. The EU's data protection standards are rooted in the long-standing experience and legal culture that have evolved across European countries over several decades. Under EU law, data protection is recognized as an independent fundamental right. In 2009, the Lisbon Treaty conferred legally binding force upon the Charter of Fundamental Rights, thereby making it part of the EU's primary legislation[2]. This marked a new stage in the legal development of data protection and significantly reinforced the fundamental right to personal data protection at the EU level through legislative means.

The Charter of Fundamental Rights applies across all areas, including the activities of law enforcement bodies. This served as the foundation for the adoption of the LED.

2. The Importance of LED

As noted, the processing of personal data by law enforcement bodies within the European Union is governed by a separate legal instrument. Unlike the General Data Protection Regulation (GDPR), which is directly applicable in all EU Member States, the LED does not have direct effect. Its implementation requires each Member State to adopt corresponding national legislation to ensure compliance with its provisions.

It is important to note that the LED takes into account the specific nature of law enforcement activities, providing a broader range of tools to enable competent authorities to effectively fulfil the functions and duties assigned to them by law. Overall, the Directive establishes a comprehensive framework within the European Union to ensure a high level of personal data protection, while recognizing the operational particularities of law enforcement bodies. Its scope extends to the processing of personal data carried out wholly or partly by automated means. Furthermore, the Directive also applies to the processing of personal data, whether or not by automated means, that form part of a filing system or are intended to be included in such a system.[3] The protection of personal data should not depend on the type of technology used, so as to prevent any circumvention of the Directive's requirements. Accordingly, the Directive applies both to data processed by automated means and to data processed by non-automated means for the purpose of subsequent inclusion in a filing system. With regard to its scope, the Directive establishes a minimum standard for Member States of the European Union, without precluding them from adopting higher standards of protection. Consequently, the LED applies to the activities of the competent authorities of EU Member States in relation to the

[2] Charter of Fundamental Rights of the European Union. Official Journal of the European Union C 326, 26.10.2012.

[3] LED, Article 2, Paragraph 2.

processing of personal data carried out for the purposes of the prevention, investigation, detection, or prosecution of criminal offences, as well as the execution of criminal penalties. Its scope also extends to processing activities conducted for purposes related to public security, the protection against threats, and the prevention of such threats.

It is important to note that when law enforcement bodies process personal data for purposes other than those specified in the LED, the EU General Data Protection Regulation (GDPR) applies. For instance, if a border guard apprehends an individual who has unlawfully crossed the border of an EU Member State and such conduct constitutes a criminal offence, the processing of that individual's data will be governed by the LED, provided that the police initiate a criminal investigation. However, if the same individual subsequently applies for asylum, the processing of their personal data must be carried out in accordance with the provisions of the GDPR, as the data is then processed for a different purpose—one unrelated to the prevention or investigation of crime.

3. Main Purposes of LED

In general, the primary objective of the LED is to enhance the protection of individuals' fundamental rights in the areas of policing and criminal justice, while also improving the exchange of personal data among EU Member States. This entails both a positive obligation on the part of the state to safeguard the fundamental rights and freedoms of individuals—particularly the right to personal data protection—and a negative obligation not to obstruct the exchange of personal data within the EU by law enforcement bodies, provided that such data transfers are required under EU or Member State law and are not otherwise restricted for reasons relating to the protection of individuals. For the Directive to apply, both its personal and material scope must be met. In other words, the processing must be carried out by a competent law enforcement body (personal scope) and must serve the purposes of the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security (material scope).[4]

The legislation of EU Member States may vary in terms of which acts are classified as criminal offences. An act that constitutes a crime in one Member State may be treated as an administrative offence in another, or may not be considered a criminal offence at all due to its low level of risk. Criminal law is deeply embedded in the domestic political, social, and constitutional framework of each country and is often associated with the state's sovereign authority. For example, the minutes of the Commission's expert group meetings during the drafting of the Directive reveal that there was no consensus among Member States on how to distinguish a criminal offence from an administrative or minor offence in those jurisdictions where such classifications do not exist. Ultimately, the European Commission determined that

[4] *Sajfert J., Quintel T.*, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, 2017, 3.

Member States may apply the concept of a criminal offence as defined under their national legal systems when implementing the Directive.[5]

This issue is particularly significant because it raises the risk of an overly broad interpretation of the LED under the justification of combating crime. Technological advancements now enable competent authorities to collect personal data more easily through modern surveillance tools and databases, as well as by accessing data collected by private individuals. Any ambiguity in the scope of the Directive may give rise to critical questions regarding the protection of the rights of individuals whose data could be processed on this basis. This also encompasses the potential risk of crime or harm, which may be invoked to justify the application of the standards set out in the LED.

One of the purposes of data processing under the Directive is also the execution of a sentence. In this context, attention must be given to the nature of the sentence, as the term may not be limited solely to criminal sentences, but could also encompass certain administrative and/or disciplinary sanctions. This distinction may be further clarified in national legislation, given that some administrative or disciplinary measures can closely resemble the execution of a criminal sentence. For instance, when a convicted individual commits a disciplinary offence while serving their sentence, it becomes challenging to exclude the application of the provisions established by the LED when imposing the corresponding disciplinary sanction.

The issue of public security should be considered separately from the prevention and investigation of crime, particularly when there is a need to protect it from potential threats. The inclusion of public security has effectively broadened the scope of the Directive, creating a risk that it may extend beyond criminal matters to encompass a wide range of data processing activities. Under the national legislation of certain Member States, the concept of public security may include the protection of other interests, such as public health. The addition of this provision to the LED has generated differing opinions and has been subject to criticism in the academic literature. Scholars have noted that "the expansion of the scope of the Directive inevitably raises questions regarding the protection of individual rights, as well as the necessity and proportionality of such a legislative approach." In light of these concerns, some authors recommend removing the phrase "including the protection against and prevention of threats to public security" from Article 1 of the Directive.[6]

4. Principles Related to Data Processing

Despite the unique nature of law enforcement activities, which may require a different approach to data processing compared to other public bodies, law enforcement bodies remain bound by the fundamental principles of data protection.

[5] *Kosta E.,* Boehm F., The EU Law Enforcement Directive (LED): A Commentary, 2024, 60.
[6] Ibid.

Personal data collected by these authorities must comply with the principles of legality and fairness, purpose specificity and proportionality, as well as accuracy and security.[7]

The principle of legality requires that personal data be processed by an authority acting in accordance with a task established by law. Beyond ensuring that law enforcement activities are grounded in legal authority, it is essential that the applicable legislation is accessible to the public and meets the criterion of transparency. This requirement is particularly critical in the context of covert law enforcement operations. Accordingly, the scope of covert actions, as well as the timelines and procedures for their implementation, must be clearly defined in legislation. Furthermore, mechanisms for the supervision of the relevant authority must be in place following the execution of such covert actions.

With regard to the observance of the principle of fairness by law enforcement bodies in the processing of personal data, although fairness is a broadly defined concept, in this context it primarily concerns the equitable application of procedural rules. Decisions affecting the data subject should, as far as possible, involve the individual at an early stage. The data subject should have access to relevant documents, and their position should be able to influence the decision-making process, including through the availability of an appropriate right of appeal. The specific nature of law enforcement activities must also be taken into account to ensure that procedural safeguards do not impede the fight against crime. However, this consideration does not negate the obligation to provide individuals with the means to protect their rights, including the provision of timely and appropriate information.

Personal data must be collected for specified, explicit, and legitimate purposes within the scope of the Directive and must not be processed for purposes incompatible with the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, including the protection against and prevention of threats to public security. These purposes, by themselves, are too broad to satisfy the principle of purpose limitation. It is therefore essential that the purpose be clearly defined, so that the rationale for processing specific data is transparent. A general reference to the needs of law enforcement bodies alone cannot constitute a legitimate purpose. In the case of Inspektor v. Inspektorata kam Visshia sadeben savet, the Court of Justice of the European Union clarified that when data collected for the purpose of investigating a crime are later used for prosecuting a criminal offence, the two activities constitute distinct purposes if the initial criminal investigation has been unsuccessful.[8]

Closely related to the principle of purpose limitation is the principle of data minimization, which requires that personal data no longer relevant to the purposes of processing be destroyed. This principle also mandates that data should not be retained for longer than necessary for the purposes for which they were originally collected,

[7] LED, Article 4.
[8] CJEU, C-180/21, Inspektor v. Inspektorata kam Visshia sadeben savet, (2022), 44.

except where retention is justified for other legitimate purposes, such as archiving or statistical analysis. [9]

Alongside the lawful acquisition of data, ensuring the security of the collected data is equally important, a principle explicitly recognized in the LED. This is particularly critical given the specific nature of law enforcement activities, as these authorities often handle special categories of data, the disclosure of which could cause significant harm to data subjects, both in terms of personal data protection and the violation of privacy rights. To mitigate these risks, competent authorities should establish specific regulations governing access to data, with access granted strictly on a need-to-know basis. It must also be possible to track who has accessed the data and for what purpose, using effective control and monitoring mechanisms..

One of the fundamental principles established in the EU's General Data Protection Regulation (GDPR) is transparency.[10] The LED does not explicitly establish transparency as a standalone principle. However, paragraph 26 of its preamble emphasizes that any processing of personal data must be lawful, fair, and transparent with respect to the individuals concerned, and must be carried out solely for purposes defined by law. This requirement does not, however, preclude law enforcement bodies from conducting activities such as covert operations or video surveillance.[11] In addition, Article 12 of the LED addresses the obligation to inform the data subject, requiring that information be provided in a concise, clear, and easily accessible manner.[12] This provision of the Directive differs from the EU's General Data Protection Regulation in that the Data Controller is not required to proactively inform the data subject but only to make the relevant information available. Furthermore, the Directive provides exceptions to the right to information and the right of access where the exercise of these rights could impede the effective functioning of law enforcement bodies.[13] We will discuss this issue in more depth in the next chapter..

In conclusion, the principles established under the Directive differ substantially from the corresponding provisions of the EU General Data Protection Regulation. They are specifically tailored to address the operational needs of law enforcement bodies and the particular nature of their data processing activities. This approach aligns with the recognition, set out in Declaration No. 21 annexed to the Treaty of Lisbon, of the distinctive character of data processing carried out by police and criminal justice authorities.[14] On the other hand, these differences may be viewed as diminishing the overall level of protection afforded to data subjects under EU law and as granting excessive discretion to police and criminal justice authorities compared to other public sector entities governed by the EU's General Data Protection Regulation.

[9] Fundamental Rights Agency (FRA), Council of Europe (CoE), European Court of Human Rights (ECHR). Handbook of European Data Protection Law, 2018, 143-144.
[10] General Data Protection Regulation, article 5, Paragraph 1(a).
[11] Preamble to the LED, paragraph 26.
[12] Ibid, Article 12.
[13] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary. 2024, 147.
[14] Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (2007). 12007L/AFI/DCL/21.

5. Rights of Data Subjects

In Europe, data subject rights constitute a fundamental element of data protection legislation. The overarching objective of the LED is to reinforce these rights. To this end, the Directive requires EU Member States to establish mechanisms ensuring that data controllers are obligated to facilitate the effective exercise of data subject rights.

5.1. Right to Access Information

The data subject's right of access to information encompasses the right to obtain, in an intelligible form, details regarding the controller, the purposes of the processing, the right to lodge a complaint with a supervisory authority, and the right to request access to, rectification, erasure, or restriction of the processing of their personal data. In addition, in specific cases and for the purpose of exercising their rights, the data subject must be informed of the legal basis for the processing and the retention period of the data, insofar as such additional information is necessary in the given circumstances to ensure the fair processing of the data subject's personal data.[15] However, the right to receive information is not absolute and may be subject to certain restrictions. These limitations arise from the specific nature of law enforcement activities, allowing the state to introduce exceptions regarding the provision of information to data subjects. It is therefore essential to maintain an appropriate balance between the individual's right to information, the necessity of providing information concerning them, and the need to avoid jeopardizing the operational effectiveness of law enforcement bodies, particularly in cases where data are processed through covert means. The European Court of Human Rights, in "Roman Zakharov v. Russia", emphasized that notifying an individual following the completion of covert investigative measures is an integral element of ensuring the effectiveness of judicial protection. The Court noted that Russian legislation did not provide effective legal safeguards against covert surveillance measures in situations where no criminal proceedings had been initiated against the person subjected to surveillance. Consequently, the Court found that "the national legal provisions governing the surveillance of communications do not provide adequate and effective guarantees of protection against arbitrariness and the risk of infringement of rights." The Court further held that the relevant legal framework failed to meet the "quality of law" requirement and did not ensure that the interference was limited to what was "necessary in a democratic society".[16]

Under the LED, EU Member States are permitted to restrict a data subject's right to access information, provided there is a legal basis for such restrictions, a legitimate interest, and that the interference is both necessary and proportionate in a democratic society. Such restrictions are justified where there is a risk of obstructing law

[15] LED Article 13, Paragraph 2.
[16] ECtHR, Roman Zakharov v. Russia, (Application no. 47143/06), VII.

enforcement activities, and where they are essential for the prevention, investigation, prosecution, or execution of criminal penalties, as well as for the protection of public and national security and the rights and freedoms of others.[17]

In summary, the objective of the LED in this regard is to ensure that individuals are informed about the processing of their personal data, thereby protecting them from potential misuse. However, this right may be subject to restrictions, but only to the extent strictly necessary.[18]

5.2. Right to Access Data

To protect the rights of data subjects, the LED also establishes the right of access, which entitles individuals to obtain access to the data processed and stored about them, as well as to be informed of the categories of such data, the purposes of the processing, and the legal basis confirming the lawfulness of the processing of their information.[19] Where possible, the data subject should be provided with information regarding the frequency of processing and the transfer of data, including details of to whom and where the information has been transferred and who the recipients are. The data subject also has the right to obtain from the Data Controller the rectification, erasure, or restriction of the processing of their data, as well as the right to lodge a complaint with a supervisory authority.[20] The purpose of Article 14 of the LED is to ensure that the Data Controller facilitates access to data relating to the data subject in an intelligible and easily accessible form, where such data are being processed.

According to the European Court of Human Rights, the State's positive obligation under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms requires it to establish an effective and accessible procedure enabling individuals to obtain all relevant information necessary for specific purposes.[21] However, it should be noted that the right of access to information is not absolute. In this case as well, a balanced approach is required, taking into account the needs of law enforcement bodies, so that the disclosure of information does not interfere with the primary objectives of their activities. Accordingly, the Directive, by way of exception, establishes the grounds for restricting this right and, in such cases, imposes an obligation on the controller to document the decision.[22] Restrictions on the right of access may be imposed depending on the circumstances of each individual case. Furthermore, when the right of access is restricted in whole or in part, four conditions must be cumulatively fulfilled:

First, there must be a legal basis. The state may adopt legislative measures, through amendments to the relevant legal acts, to restrict the exercise of the right of

[17] LED Article 13, Paragraph 3.
[18] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary, 2024, 256.
[19] LED, Article 14.
[20] Ibid.
[21] ECtHR, Yonchev v. Bulgaria (Application no. 12504/09), 50.
[22] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary, 2024, 284.

access. Naturally, these legal acts must be accessible to the concerned individuals and meet the criteria of transparency.

The second condition requires that the restriction of access to data must not be indefinite. It should be limited in time and scope, thereby satisfying the test of necessity and proportionality in a democratic society.

The third condition is the obligation to respect the rights and interests of others, which are guaranteed, among other things, by the legal acts adopted by the European Union and the Council of Europe.

The fourth condition for restricting access to data is that such a restriction must serve to prevent the obstruction of a lawful inquiry, investigation, or proceeding. It must aim to ensure the prevention, detection, or investigation of crime, the prosecution or execution of criminal penalties, as well as the protection of public and national security and the safeguarding of the rights of others.[23] The European Court of Human Rights also recognizes that the right to access information may be subject to restrictions. In particular, in "Segerstedt-Wiberg and Others v. Sweden", the Court acknowledged the legitimate existence of intelligence services and the permissibility of covert surveillance of citizens, provided that such measures are strictly necessary for the protection of democratic institutions under the Convention. Furthermore, the Court emphasizes that the state's interest in safeguarding national security and combating terrorism must be balanced against the degree of interference with the right to respect for private life.[24]

The fifth purpose relates to the protection of the rights and freedoms of others. In this context, it primarily concerns safeguarding data obtained by law enforcement bodies during the course of an investigation, which may include the personal data of potential victims, witnesses, or other involved individuals[25]. The data subject has the right to be informed of any restriction on access to their data, along with the reasons for such restriction, provided that disclosure does not compromise the achievement of the aforementioned objectives, thereby enabling the individual to challenge the decision if necessary.

5.3. Rectification, Erasure and Restriction of Data Processing

To protect the rights of data subjects, the Directive also provides for mechanisms such as the rectification, erasure, and restriction of data processing.[26] These mechanisms allow the data subject to respond appropriately when their personal data are processed unlawfully. The retention of inaccurate data by investigative authorities further heightens the risk of violations of the data subject's rights. The need for data rectification primarily arises when information about the individual is incorrect or factually inaccurate in law enforcement databases. For

[23] LED, Article 15.
[24] ECtHR, Segerstedt-Wiberg and Others v. Sweden (Application no. 62332/00), 88.
[25] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary. 2024, 290.
[26] LED, Article 16.

instance, biometric data about a person may be recorded incorrectly by the police, potentially causing a significant impact on their private life.

Regarding data deletion, it constitutes both a right of the data subject and an obligation of the controller, applicable when the principles or legal grounds for data processing are violated, when special categories of data have been processed unlawfully, or when deletion is required by a legal obligation. Ensuring the timely deletion of data is also crucial. Notably, the European Court of Human Rights has recognized a violation of the right to privacy in cases where information about suspects was retained in police databases for periods exceeding those prescribed by law.[27] Instead of erasing the data, the controller is required to restrict its processing when the authenticity of the data is disputed and its accuracy cannot be verified. In such cases, the controller must inform the data subject before the restriction of processing is lifted, or when the processing of the data is necessary for evidentiary purposes.

It is important to note that the rights of the data subject are not absolute. Their exercise must not impede the legitimate functions of law enforcement bodies. Data subject rights may also be restricted to achieve the same objectives as those applicable to limitations on the right of access to data.[28]

5.4. Right to Indirect Access to Data

To ensure the effective exercise of data subject rights, the Directive provides additional safeguards in situations where the individual's access to, rectification of, or erasure of information is restricted. The purpose of this mechanism is to maintain a balance between the rights of the data subject and the operational needs of investigative authorities. If the data subject is denied direct access to, rectification of, or erasure of their data by the controller, they are entitled to obtain indirect access through the national supervisory authority. This includes the right to have the supervisory authority verify the lawfulness of the data processing. The controller is responsible for informing the data subject of this right, and the supervisory authority must communicate the results of the verification to the data subject, as well as explain their right to seek judicial remedy.[29]

5.5. Data Processing in Accordance with National Legislation

The Directive grants EU Member States the right to access, rectify, and erase information, as well as to restrict its processing, in accordance with national law, within the context of criminal investigations and judicial proceedings. This includes, for example, witness statements, personal data obtained during searches, and information collected through covert surveillance.[30] This underscores the importance

[27] ECtHR, S. And Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04), 119, 124.
[28] LED, Article 16.
[29] ibid, Article 17.
[30] ibid, Article 18.

of state sovereignty in the conduct of investigations and judicial proceedings. However, this legal authority does not entitle states to interfere with or unduly restrict the rights of the data subject. On the contrary, national legislation in the relevant field must provide guarantees for the protection of the data subject's rights, irrespective of the specific legal framework in place.[31] In this context, states may enjoy greater legal and technical flexibility; however, this flexibility must not come at the expense of the data subject's rights. Instead, it should be exercised through the introduction of minimal safeguards within national legislation. Although the purpose of this paper is not to provide a detailed comparison between Georgian legislation and the LED, it is possible to discuss, in general terms, the extent to which national data protection laws align with the objectives of the Directive. The fact that the Law of Georgia "On Personal Data Protection" does not apply to the processing of data classified as state secrets, whether by semi-automatic or non-automatic means[32], for the purposes of crime prevention, investigation, criminal prosecution, operational-search activities, and the protection of public order, indicates a potential incompatibility with the LED.

6. Conclusion

This paper examined the significance of the LED and analysed the primary objectives underlying its adoption. It also explored the data processing principles established by the Directive. Particular emphasis was placed on the rights of data subjects when law enforcement bodies process personal data for the purposes of crime prevention, investigation, prosecution, and execution of sentences, as well as for the protection of public and national security. Throughout the study, it was highlighted that, given the specific nature and sensitivity of personal data processing in the criminal justice context, it is necessary to establish rules distinct from the general legal framework for data protection. At the same time, it was emphasized that any interference with human rights under this regulatory framework must be justified, ensuring a balance between, on one hand, the rights of the data subject, and on the other, the effective functioning of law enforcement bodies.

Of course, protecting public security and preventing or investigating crime are important objectives; however, these goals must not be pursued at the expense of violating human rights. In this context, the state bears a particular responsibility to achieve both objectives through balanced measures, including the implementation of distinct data protection rules tailored to the criminal justice sector. Consequently, despite the specific functions of law enforcement bodies, both the general legal framework for data protection and the specialized data protection regime applicable to these authorities must fully respect the requirements of the Charter of Fundamental Rights of the European Union.

[31] *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary, 2024, 322.
[32] Law of Georgia "On Personal Data Protection", 3144- XIმს-Xმპ, 14/06/2023, Article 2.

Bibliography:

1. Charter of Fundamental Rights of the European Union. Official Journal of the European Union C 326, 26.10.2012.
2. Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (2007). 12007L/AFI/DCL/21.
3. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
4. Fundamental Rights Agency (FRA), Council of Europe (CoE), European Court of Human Rights (ECHR). Handbook of European Data Protection Law.
5. Law of Georgia "On Personal Data Protection" 3144- XIმს-Xმპ, 14/06/2023.
6. *Kosta E., Boehm F.,* The EU Law Enforcement Directive (LED): A Commentary, 2024.
7. *Sajfert J., Quintel T.,* Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, 2017.
8. CJEU, C-180/21, Inspektor v. Inspektorata kam Visshia sadeben savet, (2022).
9. ECtHR, Yonchev v. Bulgaria (Application no. 12504/09), 2017.
10. ECtHR, Roman Zakharov v. Russia, (Application no. 47143/06). 2015.
11. ECtHR, S. And Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04), 2008.
12. ECtHR, Segerstedt-Wiberg and Others v. Sweden *(*Application no. 62332/00), 2006.

Pam Dixon*

Group Privacy, Data and AI: Collective Forms of Privacy and Its Relationship to Technology and Policy Frameworks

Collective privacy refers to the privacy interests of a group of people. As AI systems have advanced in capacity to analyze and segment people into groups with predictable behaviors, collective privacy has become increasingly relevant. However, there is a governance gap: while some indigenous governance frameworks such as those of the Māori acknowledge a right to collective privacy, the majority of privacy laws effectuate privacy primarily at an individual level, not a collective level. Europe's GDPR, adopted in some form in most regions of the world, exemplifies an individual privacy approach. This paper defines group privacy and analyzes the complex socio-technical environments underlying the collective privacy gap. The paper examines key case studies highlighting diverse aspects of collective privacy: the Māori algorithm charter with the New Zealand government, the All of US genetic data biobank policies, and the European Court of Human Rights case Lewit v. Austria.

Keywords: *Collective privacy, group privacy, GDPR, Artificial Intelligence, genetic privacy, indigenous governance, Māori algorithm charter, Lewit v. Austria.*

* Founder and Executive Director, World Privacy Forum.

1. Introduction

This paper explores concepts and applications of privacy in the context of groups and proposes a definition of the term *collective privacy* or *group privacy* as "those privacy interests that are held by or applicable to a definable group of people." Collective privacy is emerging as an issue of note for several reasons, one of them being that gaps in protections for group interests in privacy are becoming more visible as technology advances. Specifically, the dominant global privacy norms that focus on individual privacy rights, when contextualized in a world increasingly suffused with high volumes of data, AI, and machine learning analysis which can create, impact, and predict groups [1] in many ways, is exhibiting systemic gaps regarding the protection of collective privacy interests.

Privacy as a theory and doctrinal matter regarding individuals and privacy-related rights ascribed to individuals has been written about extensively.[2] However, collective privacy has been underrepresented in the dominant scholarly literature both about privacy and about collectivity. [3] A critically important body of scholarly, legal, and other work on collective or group privacy does exist. The clearest affirmative articulations of collective privacy at this time may be found in work relating to indigenous groups globally, and within the national and subnational tribal frameworks across a range of jurisdictions. Important examples include the U.S. Indigenous Data

[1] The concept of a group has been studied in multiple disciplines, including mathematics, physics, and social science, among others. This paper utilizes Campbell's postulation of *entitativity* (1958), later validated and refined by Lickel et al (2001) as a primary theoretical basis for determining the quality of cohesiveness of a group. When a cohesive group is formed, Campbell found that it will exhibit a range of quantifiable characteristics that determine its proximate level of entitativity, or "groupiness." Entitativity and its contribution to this analysis of collective privacy is discussed in more detail in this paper. See text and footnotes 11-15.

[2] There is an abundant and excellent literature on the complex topic of the definition of privacy. See: *DeCew J.,* Privacy, Stanford Encyclopedia of Philosophy, 2018; *Gellman R.,* Fair Information Practices: A Basic History, 2025, <http://dx.doi.org/10.2139/ssrn.5348107> [12.11.2025]; *Bamburger K. A., Mulligan D.,* Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, Cambridge: MIT Press, 2016; *Solove D.,* Understanding Privacy, Cambridge: Harvard University Press, 2008; *Solove D.,* Against Privacy Essentialism, GWU Law School Public Law Research Paper, 2025-19; *Allen A. L.,* Presidential Address, The Philosophy of Privacy and Digital Life, 93 Proceedings of the American Philosophical Association, 2019, 21-38.

[3] Collectivity is a broad topic with multiple branches of inquiry. Collective judicial action is analyzed, for example, in the large body of scholarship regarding Rwanda's Gacaca Court, which in the period from 2001 to 2012 processed almost 2 million cases related to the 1994 Rwandan genocide. See: *Megwalu A., Loizides N.,* Dilemmas of Justice and Reconciliation: Rwandans and the Gacaca Courts, African Journal of International and Comparative Law, 2010, <https://ssrn.com/abstract=1406863> [12.11.2025]. Collective bargaining is another large branch of inquiry; see: *Court de le A.,* Stabilising Collective Agreements in Continental Europe: How Contract Law Principles Reinforce the Right to Collective Bargaining, Oñati Socio-Legal Series, Vol. 9, No. 1, 2019. The extensive literature examining broader theories and practices regarding collectivity does not usually address *collective privacy* as this paper defines it. However the broader literature on collectivity is nevertheless an important aspect of understanding the ways collectivity may be expressed.

Sovereignty Network [4] and the Māori Data Governance Model, Te Kāhui Raraunga, and charter, Te Mana Raraunga Charter, among others. [5] [6] [7] [8]

In particular, the Māori literature and work around collective privacy is critically important as the ideas around collective privacy, and even the collective quality of certain data, is addressed directly. Kukutai explains that in the Māori model, collective rights may in some cases prevail over individual rights. She also notes that certain data have a "clear collective dimension," a category in which she includes DNA and genomic data, among other data types.[9] It is noteworthy that the Māori data governance framework Te Kāhui Raraunga, which is a formal treaty with the government of New Zealand, has specifically articulated collective privacy in the context of AI, delving deeply into how algorithms and other aspects of AI will be addressed in the Māori context.

2. What Constitutes a Group?

One of the challenges of collective privacy is definitional; ideas around collective or group privacy raise many questions about how the groups themselves are defined, or which groups would benefit from collective privacy protections, or how that could be fairly decided, and by whom. How to define a group is a foundational question that has to be addressed systematically when approaching the concept of collective

[4] Indigenous Data Sovereignty, or IDSov, is a significant movement across multiple jurisdictions and regions. Definitions about indigenous data sovereignty can vary regionally and culturally. Data sovereignty as it relates to collective privacy is the focus of this paper, however, the ideas of data sovereignty encompass much broader issues that extend beyond the scope of this paper. See: The Global Indigenous Data Alliance, <https://www.gida-global.org> [12.11.2025] .

[5] Te Kāhui Raraunga, <https://www.kahuiraraunga.io/maoridatagovernance> [12.11.2025]. See also Te Mana Raraunga Charter, <https://www.temanararaunga.maori.nz/tutohinga> [12.11.2025].

[6] For example, the Māori have distinct and well-developed concepts of collective privacy enshrined in their culture as well as tribal laws. The Māori consider privacy to be a collective right, to be effectuated collectively. There is a detailed and nuanced literature around concept of collective privacy for the Māori. This paper introduces the concept and develops it in contrast to the dominant individual concepts of privacy. For a detailed articulation of what indigenous peoples consider to be collective privacy, see, e.g., *Quince K., Houghton J.,* Privacy and Māori Concepts" in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136.

[7] This paper discusses the indigenous and multilateral literature regarding collective privacy in detail in the case study analyses in this paper.

[8] The Māori consider privacy to be a collective right, to be effectuated collectively. There is a detailed and extremely nuanced literature around this concept of collective privacy for the Māori. To begin to understand collective privacy, it is essential to understand the indigenous people's philosophy regarding collective privacy. See, e.g., *Quince K., Houghton J.,* "Privacy and Māori Concepts" in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136, <https://researchspace.auckland.ac.nz/handle/2292/67023> [12.11.2025].

[9] *Kukutai T.,* Indigenous Data Sovereignty – a New Take on an Old Theme, Science, Vol. 382, No. 6674, 2023. As quoted in the article, Kukutai explains collectivity in indigenous frameworks: "All of the CARE principles (collective benefit, authority to control, responsibility, and ethics) speak directly to collective rights and responsibilities. The Māori data sovereignty principles go one step further, stating that in some data contexts, 'collective Māori rights will prevail over those of individuals.' " The CARE principles Kukutai references were crafted by GIDA, the Global Indigenous Alliance. See: Care Principles, GIDA, <https://www.gida-global.org/care> [12.11.2025].

privacy. To accomplish this, the research for this paper examined a broad literature on groups.

To begin with, an illuminative body of work exists in the scientific literature about what constitutes a group. This literature includes mathematical representations and concepts of groups, which date back to the 1700s. In abstract algebra, "group theory" simply means the study of groups, which in the mathematics context are complex algebraic structures.[10] Algebraic group theory has influenced physics as well as set theory, both of which contribute interesting ideas to the study of groups, group dynamics, and other group structures. Physics incorporates group theory structures widely, particularly in the context of symmetry or invariance.[11] Group theory is considered by some theoretical physicists as the dominant organizing principle of modern physics.[12]

A key scholarly literature in social science regarding groups is *entitativity*, which is a core term of art regarding what constitutes a group of people that are bounded together in some way. Sociologist Donald Campbell introduced the term in 1958 to describe groups that had certain common characteristics. The higher the entitativity of a group, the more cohesive and bound together the group. Lickel *et al* defined the term of art as it is now known, that is, *entitativity* is the "…degree to which a collection of persons are perceived as being bonded together into a coherent unit." [13]

Campbell proposed a set of criteria for determining if a group could be considered as an entity fit for analysis in the social sciences. These included interactivity, similarity, sharing the same goal, sharing a common fate, and having a psychological or physical boundary to the group.[14] Subsequent research has found that three of the components in particular are usually involved in entitativity: "…'essence' (the group members' similarity), 'agency' (the goals and the interaction between group members) and 'unity' (the cohesion of a group and the degree of the group importance).[15] Additionally, the groups that display qualities of entitativity tend to cluster into four types of groups, ranked from most to least entitative: intimacy groups

[10] *Dummitt D. S., Foote R. M.,* Abstract Algebra, 3rd ed., 2003. See Part I: Group Theory, chapters 1-6, Group Theory.

[11] *D'Hoker E.,* Mathematical Methods in Physics - 231B - Group Theory, Mani L. Bhaumik Institute for Theoretical Physics, Department of Physics and Astronomy, Course Notes, 2019, <https://www.pa.ucla.edu/faculty-websites/dhoker-lecture-notes/graduate-courses/group-theory.pdf> [12.11.2025].

[12] Ibid.

[13] *Lickel B., Hamilton D.L., Wieczorkowska G., Lewis A., Sherman S.J., Uhles A.N.,* Varieties of Groups and the Perception of Group Entitativity, Journal of Personality and Social Psychology, 78(2), 2000, 223–246. See page 224 for the definition.

[14] *Campbell D. T.,* Common Fate, Similarity and other Indices of the Status of Aggregates of Persons as Social Entities, Behavioral Science, 1958, <https://doi.org/10.1002%2Fbs.3830030103> [12.11.2025].

[15] As quoted in: *Agadullina E. R., Lovakov A. V.,* Understanding Entitativity: Are There Real Differences between Approaches? Journal of the Higher School of Economics, 2017.

(such as family and friends), task groups, social categories (gender, race), and loose association groups (for example, people who like certain types of music).[16]

To explore collective privacy in depth across similar groups, this paper discusses and analyzes three case studies focused on groups that demonstrate high entitativity per Lickel *et al* and Agadullina *et al.* The first case study focuses on indigenous collective privacy frameworks, including the Māori algorithmic charter, a major part of the collective privacy literature. The second case study involves a large U.S. National Institutes of Health biobank called the All of Us program, which has set a goal of collecting 1 million genetic samples for research. The All of Us program undertook an extensive review in 2021 regarding the effectiveness of consent provisions under the current U.S. law to protect the privacy of DNA contributions made by U.S. tribal members. The findings of the NIH review raised extensive and complex issues, and noted that broad consent for genetic data donated to the All of Us biobank program would not provide effective privacy protections for tribal members under the existing law. The report raised the issue of what it called "identitativity" of an individual research subject to a specific tribal group, despite privacy protections and deidentification measures being in place.

The third case study involves a collective group of holocaust survivors who were liberated from the Mauthausen concentration camp in 1945 and who were still alive in 2016. A publication in Austria defamed these survivors as a collective group, and the survivors subsequently brought a case before the Austrian courts. The survivors were denied standing because they were seen as a collective group without individual privacy rights. This case was eventually brought before the European Court of Human Rights (ECHR). The ECHR's decision and arguments in this case study speak directly to important aspects of collective privacy and reveal stark gaps in protections for collective privacy, even in a country with strong data protection laws in place.

Prior to discussing the analysis of the case studies, it is essential to contextualize the discussion of collective privacy in the current technical, social, and legal contexts as applied within the dominant practices and laws today.

3. Collective Privacy and the Impact of AI and Machine Learning Ecosystems on Privacy and Data

The emergence of advanced forms of AI and deep learning[17] creates significant pressures on policies regarding the use of data broadly, and aggregated or deidentified data specifically. Regarding the application of AI to group concepts, there is already a

[16] *Agadullina E. R., Lovakov A. V.,* Understanding Entitativity: Are There Real Differences between Approaches? Journal of the Higher School of Economics, 2017.

[17] *Vaswani A., Shazeer N., Parmar N., Uszkoreit J., James L., Gomez A. N., Kaiser L., Polosukhin I.,* Attention is All You Need, arXiv:1706.03762v7 [cs.CL], <https://doi.org/10.48550/arXiv.1706.03762> [12.11.2025]. The paper was first presented at the 31st Conference on Neural Information Processing Systems (NIPS 22017), Long Beach, CA, USA. It is an influential landmark paper in the history of AI. See also: *Murgia M.*, Generative AI Exists Because of the Transformer, This is how it: Writes, Works, Learns, Thinks and Hallucinates, Financial Times, 2023.

body of extensive work. Entitativity criteria are already widely used as a core concept in sophisticated social research regarding groups;[18] entitativity research is also being applied in additional domains of research that stem from nascent areas of AI. For example, applying AI and deep learning-based research using the field of topological data analysis to the investigation of social group cohesion can be used to predict the composition and behavior of groups.[19] One exemplar in this area is research that combines entitativity with AI-enabled analysis to determine virtual and physical characteristics of high-entitativity groups and to forecast the impacts of these groups on others outside the group.[20] Large open data sets such as SALSA,[21] when combined with entitativity analysis results in rich and deep research about groups, many of which raise substantial ethical and privacy issues. With the advent of advanced reasoning Large Language Models or LLMs,[22] the ease of creating programming code to run entitativity or other group analysis against large datasets of individuals at scale has raised the importance of a systematic evaluation of the risks to collective privacy that can be seen emerging today.[23]

There is significant consensus-driven multistakeholder work that discusses in various ways the intersections of privacy and and advanced forms of machine learning and AI. These works identify risks and outline general principles. Important exemplars include UNESCO's Recommendation on the Ethics of Artificial Intelligence, which applies to all of its 194 member states.[24] OECD's AI Principles are also important. These principles were the first intergovernmental standard on AI to be published. The principles were developed by a consensus body of its member governments along with its formal advisory bodies, which include civil society, business, standards development organizations, and additional stakeholders. A group of AI experts were gathered by OECD in 2018 to engage with this process to ensure technical accuracy and depth. The OECD AI Principles were ratified in 2019 and updated in 2024.[25] However, while valuable and important, this early work by UNESCO and OECD does

[18] Bernado F., *Palma-Oliveira J. M.,* Tell me Where you Live…How the Perceived Entitativity of Neighborhoods Determines the Formation of Impressions About their residents, Frontiers in Psychology, 2022.
[19] *Liang C., Chen V., Shah J., Andrist S.,* Converting Spatial to Social: Using Persistent Homology to Understand Social Groups, ACM International Conference on Multimodal Interaction (ICMI), Canberra, Australia, 2025.
[20] *Bera A.,* Data Driven Modeling of Group Entitativity in Virtual Environments, VRST 2019, Tokyo Japan <https://arxiv.org/pdf/1810.00028> [12.11.2025].
[21] *Alameda-Pineda X.,* SALSA: A Novel Dataset for Multimodal Group Behavior Analysis, IEEE Trans Pattern Anal Mach Intell, 2016.
[22] Large Language Models or LLMs are architected utilizing transformer models. LLMs are often characterized by the exceptionally large datasets used to train the models. See Wikipedia entry "Large Language Model," <https://en.wikipedia.org/wiki/Large_language_model> [12.11.2025].
[23] In one example, a multitasking convolutional neural network was used to predict the Group Cohesion Score of groups of people using visual images of the group. *Gosh S.,* Predicting Group Cohesiveness in Images, 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 2019, 1-8.
[24] Recommendation on the Ethics of Artificial Intelligence, UNESCO, 2022, <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence> [12.11.2025].
[25] OECD AI Principles, 2019 (Ratified), 2024 (updated).

not incorporate a robust analysis of AI impacts on groups in regards to privacy specifically.

An early feasibility study from the Council of Europe's (COE) Ad hoc Committee on Artificial Intelligence, CAHAI, investigated possible elements of a legal framework on AI. In this study, the COE specifically discussed the impact of AI on groups, noting that groups may experience discrimination based on AI analysis. The conception of "groups" in the study was not differentiated according to group cohesion, and did not include a specific analysis of advanced AI techniques impacting group privacy, however, the study did consider utilizing anti-discrimination laws as a possible way of addressing group harms, where AI systems are being used to create new groups. Ultimately, the Council of Europe in its final version of the Framework Convention on Artificial Intelligence did not include group concepts, but the discussion of group action related to AI is still an important contribution.[26] [27]

Another important contribution by the Council of Europe is contained in its Recommendation on the protection of individuals with regard to automated processing of personal data in the context of profiling, where the Council included a discussion of AI and groups in this specific context, noting:

1 i-j:
"…High-risk profiling" may refer, inter alia, to:
…profiling operations that entail legal effects or have a significant impact on the data subject or on the group of persons identified by the said profiling;"

2.6:

"…Profiling must not result in discrimination against individuals, groups, or communities."

B. 78:

"…. AI applications should allow effective control, by the data subjects and groups concerned, of the effects of their applications on individuals, groups and society."

8.5:

[26] Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study, 17 December 2020, <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> [12.11.2025]. See for example Paragraphs 20, 25, and discussion in note 15 regarding discrimination. CAHAI was the forerunner to the CAI, which completed what became the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law. See note 26.

[27] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, 5 September 2024.

> "The field of inquiry of supervisory authorities should be broadened to include collective and societal risks. Their opinions should mention such risks and their decisions should take them into consideration."[28]

The COE defined what it meant by AI, but it did not specifically define what constitutes a group, nor did it set out a specific definition of group privacy or collective privacy. It is an important contribution, but it does not provide a complete literature on the topic. The EU AI Act also discusses the concept of groups, noting in Article 5 specific prohibited practices regarding individuals and groups. Groups are not specifically defined, and the EU AI Act does not specifically address privacy.[29]

The most completely stated policy literature that addresses and defines collective privacy directly, including but not limited to the context of AI, is primarily written by or with indigenous peoples about tribal data and tribal data laws. This literature includes legal arguments that some tribal governments possess the authority to enact data privacy laws at the tribal level. The tribal laws define what constitutes tribal data. Tsosie states:

> "…federally-recognized tribal governments do possess the authority to enact laws at the tribal level. Although jurisdictional limitations may exist, tribal laws can help inform analogous federal and state policies governing data, for example, by defining what constitutes "tribal data" and what would be appropriate ways to secure tribal consent to collection, use or disposition of such data."[30]

These ideas and approaches can be seen articulated in a number of exemplars which articulate specifically what collective privacy is, including in the context of AI; one exemplar this paper already brought forward is the Māori Data Governance Model, Te Kāhui Raraunga, and charter, Te Mana Raraunga Charter. Another examplar comes from the First Nations Principles of OCAP, which establishes how First Nations'

[28] Council of Europe Recommendation of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 3 November at the 1416th meeting of the Ministers' Deputies).

[29] EU Artificial Intelligence Act, Regulation – EU – 2024/1689. The EU AI Act is designed to funnel privacy concerns in AI to be addressed through other legislative and regulatory instruments, including the GDPR. The handoff of privacy between the EU AI Act and the GDPR is extremely complex. Notably for the topic of this paper, group concerns regarding *privacy* as defined in GDPR are not considered in the EU AI Act, which is why the AI Act is not further analyzed as a core topic in this paper. It bears stating here that in the GDPR, privacy is primarily effectuated at the individual level, not at the group level. In use case 3 in this paper, the analysis of Lewit v. Austria touches on the overarching articulation of rights at an individual level in EU legal instruments and the limitations of individual approaches in certain contexts. Because the EU AI Act does not address collective privacy, a detailed discussion of these issues vis à vis the EU AI Act and its interaction with the GDPR will be taken up in a separate paper that explores the topic further.

[30] *Tsosie R.,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019).

data and information will be collected, protected, used, or shared in Canada.[31] Despite these strong articulations of indigenous policy, the practical implementation of these policies remains a difficult challenge in the development and deployment of data governance policies, as well as deployment of AI tools and systems.

This indigenous literature regarding AI and collective privacy is immeasurably important. As discussed earlier in this paper, modern AI systems can be at odds with privacy rights generally, including emerging areas of collective privacy risks emerging in newer AI and machine learning analyses. Indigenous socio-technical approaches often stress privacy as a collective issue and not as only an individual issue; these policies comprise a core articulation of collective approaches to privacy today, as collective privacy is not yet a front-line discussion held in the dominant culture of privacy.

There is an additional body of literature developing around data, AI, and collective privacy which is being created by philosophers and technologists who do not generally reference indigenous concepts, rather they draw from their perceptions and analyses about the actions and impacts of technologies on privacy as a whole. The philosopher Alessandro Mantelero wrote about the opportunity that big data and advanced analytics provides for redefining and expanding the boundaries of data protection concepts to include group privacy rights. He writes:

> "The peculiar nature of the groups generated by big data analytics request an approach that cannot be exclusively based on individual rights. The new scale of data collection entails the recognition of a new layer, represented by groups' need for the safeguard of their collective privacy and data rights." [32]

The "new layer" Mantelero identified is an astute observation, and is substantiated by technical research in AI and entitativity.[33] However, current law that is focused on individual data rights has been constructed in such a way that collective data has been in many ways devalued as to its privacy importance. Notably, deidentified data sets are typically beyond the reach of much privacy law. This can introduce problems today when deidentified data is analyzed and/or scored and the results affect individuals. In addition, modern forms of AI can permit a variety of advanced analysis of data without deidentifying the data and without allowing anyone

[31] First Nations Information Governance Centre, *The First Nations Principles of OCAP*, https://fnigc.ca/ocap-training/.

[32] *Mantellerò A.,* From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era, 2017. Group Privacy. Philosophical Studies Series, vol 126. Springer, Cham. <https://doi.org/10.1007/978-3-319-46608-8_8> [12.11.2025].

[33] Research regarding high entitativity groups includes, for example, the definition of entitativity: *Lickel B., Hamilton D. L., Wieczorkowska G., Lewis A., Sherman S. J., Uhles A. N.,* Varieties of Groups and the Perception of Group Entitativity, Journal of Personality and Social Psychology, 78(2), 2000, 223–246. See page 224 for the definition. An example specific to AI includes: *Liang C., Chen V., Shah J., Andrist S.,* Converting Spatial to Social: Using Persistent Homology to Understand Social Groups, ACM International Conference on Multimodal Interaction (ICMI), Canberra, Australia, 2025.

to view, use, or disclose the identified data.[34] While this can be a potential privacy boon, the consequences to individuals can range from helpful to problematic. This kind of practice has meaningful implications in a world in which advanced forms of AI can achieve increasingly accurate analysis of deidentified and encrypted data which can then be applied at a group, household, or even individual level. The dominant privacy laws in place today typically favor individual privacy rights over collective privacy, and as such, often exempt deidentified data from privacy protections.

Mühlhoff and Ruschemeier articulate this problem in privacy as a consequence of predictive analytics and a lack of collective privacy protections, specifically calling their theory "predictive privacy." It is an intriguing formulation:

> "…We argue that the individualised concept of regulation, shaped by the dogma of fundamental rights, is unable to adequately capture the implications of predictive analytics. We show that predictive analytics is a problem of collective privacy and informal power asymmetries, and conceptualise the form of data power at work in predictive analytics as "prediction power". The unregulated prediction power of certain actors poses social risks, especially if this form of information power asymmetry is not normatively represented."[35]

The normative representation that is missing is that deidentified data is not typically seen as worthy of data protections. The underlying argument at the root of this perception is that collective privacy does not matter as much as individual forms of privacy. There is a basis in reality for these criticisms. For example, in the U.S., the Federal health privacy law, HIPAA, provides that protected health information regulated under HIPAA may be shared or sold if certain deidentification procedures and measures are applied. The HIPAA deidentification standard in place today dates back to the 1990s and is likely out of date in light of modern analytics and AI.[36] However, it is now a well-established practice and it would be extremely difficult to dislodge. Also in the U.S., the Fair Credit Reporting Act applies only to individuals. If, therefore, a risk score about a household uses broad demographic information and aggregate financial data without using regulated elements such as credit bureau data, Fair Credit Reporting Act rights do not apply.[37] The Court of Justice of the European Union has recently clarified certain aspects of data protections for pseudonymous

[34] *Nicholson W., Cohen G.,* Privacy in the Age of Medical Big Data, Nature Medicine 25, 2019, 37–43.
[35] *Muhlhoff R., Ruschemeier H.,* Predictive Analytics and the Collective Dimensions of Data Protection, 16.1 Law, Innovation and Technology, 2023.
[36] For example, HIPAA, the federal health privacy law, allows for the use of deidentified data when it meets certain criteria. An early foundational paper articulating how the technology was viewed at the time is: Sweeney L., Weaving Technology and Policy Together to Maintain Confidentiality. Journal of Law, Medicine & Ethics, 25, nos. 2&3, 1997, 98-110.
[37] Federal Trade Commission, Section 319 of the Fair and Accurate Credit Transactions Act of 2003: Fifth Interim Federal Trade Commission Report to Congress Concerning the Accuracy of Information in Credit Reports.

data, [38] however, direct or indirect individual identifiability of the data is still a key test of when data can be classified as personal data.[39]

The risk of reidentification of aggregate or deidentified datasets is shifting as compute power and analytical sophistication improves.[40] An additional challenge arises when data is analyzed while still deidentified, because this activity typically does not fall under current privacy laws that focus on individual rights. For example, large data pools can be analyzed and then scored using a variety of machine learning and AI techniques. The scores -- even though they contain no personally identifiable data -- can then be applied to neighborhoods, census blocks, or households.[41] Continuing this example, individuals living in neighborhoods scored as higher risk can be affected; this can occur even though the neighborhood score is an aggregate measure that did not use or reveal personally identifiable information.[42] While there can be regional variations of this process, a risk score when applied to a group of people, especially if individual data is held in the aggregate, may not be covered under any particular law. Meanwhile, aggregate data that is analyzed and scored can still act to categorize people, predict behaviors, and create a variety of impacts that can be meaningful in a range of ways, both positive and negative.

Analyzed from a purely technical point of view, AI analysis and scoring of deidentified or aggregate data (including aggregate medical data) is able to draw conclusions about groups of people. Yet the granting of individual privacy rights currently available in most privacy law does not appear to meaningfully assist the protection of collective privacy interests that might be present in some cases. This point is made eloquently by two Māori authors who writing about how non-indigenous privacy approaches differ from theirs:

> "There are discernible differences between Māori and non-Māori concerns about privacy. These different concerns were reflected in our different aspirations for the reform process. …. We contend that, while the new Act champions individualistic Western conceptions of privacy with little regard for collective

[38] ECLU:EU:C:2025:645, Case C-413/23 P, September 2025.

[39] Article 3 (6) of Regulation 2018/1725: "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." See also Article 3 (1).

[40] *Sweeney L.,* You J. S., De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data*,* Harvard Journal of Technology Science, 2015, <https://techscience.org/a/2015092901/> [12.11.2025].

[41] Dixon P., Gellman R., The Scoring of America, World Privacy Forum, 2014, <https://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf> [12.11.2025].

[42] *Testimony of Pam Dixon regarding Data brokers and the impact on financial data privacy, credit, insurance, employment, and housing, before the United States Senate Committee on Banking, Housing, and Urban Affairs*, 2019, <https://www.banking.senate.gov/hearings/data-brokers-and-the-impact-on-financial-data-privacy-credit-insurance-employment-and-housing> [12.11.2025].

conceptions of privacy, Māori may nonetheless find privacy law useful to achieve certain ends…." [43]

It is true that collective interests do not appear prominently, or in many cases, at all in Western law. This is not in dispute here. What is in dispute is the effectiveness of existing dominant privacy laws in effectuating aspects of group privacy when considering certain privacy scenarios, including those involving AI systems.[44] Dominant privacy laws and norms do not sufficiently address what indigenous communities and others need to ensure that collective forms of privacy thought and policy at the tribal and other levels are incorporated and addressed. In addition, current privacy laws also do not sufficiently address need for collective privacy interests beyond indigenous communities.

4. Individual Privacy Rights and a Brief Background of the Evolution of Privacy Law

Some additional contextualization regarding the specifics of existing privacy law and norms here is useful before discussing the collective privacy exemplars, as this paper discusses specific elements of dominant and non-dominant privacy law.

The dominant expression of privacy norms today is expressed in the broad concepts of the European-based General Data Protection Regulation, or GDPR.[45] The GDPR did not originate from a policy vacuum — rather, it is the expression of a long process of development over time. Privacy has a well-defined, deep, and instructive history.

In the late 1960s, driven to a significant degree by rapidly developing information technologies, attention to data governance,[46] data protection, and privacy began

[43] *Houghton J., Quince K.,* Privacy and Māori Concepts" in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136, <https://researchspace.auckland.ac.nz/handle/2292/67023> [12.11.2025].

[44] Gucluturk O., How to Handle GDPR Data Access Requests in AI-driven Personal Data Processing, 2024, <https://oecd.ai/en/wonk/gdpr-data-access-requests> [12.11.2025]. Also see discussion of broad consent regarding human subject research in this paper.

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[46] Data governance and privacy are related, however they are different in meaning. Even though these terms might be used in tandem, they are not interchangeable. Data governance is a comprehensive approach to the entirety of data of an organization or entitativity that ensures information is managed through the full data lifecycle. This can include data collection practices, data security, quality, documentation, classification, lineage, cataloging, auditing, sharing, and other aspects. Data privacy is a subset of data governance, and is best defined in context as forms of protecting either personal data, or the personal data of a group of people. An articulation of individual privacy may be seen in OECD's *Recommendation on Privacy* (the Fair Information Practice Principles) or in Directive 95/46/EC, 1995 O.J. (L 281) 31 and the General Data Protection Regulation. As discussed in this paper, while the overarching European conception of privacy is dominant in terms of legislation, there are other conceptions of privacy in other cultures. For example, community-based privacy norms

slowly, with small developments here and there around the world.[47] Fair Information Practices (FIPs),[48] the early core statement of data governance and privacy values started in 1973 in the United States, were restated by the Organization of Economic Cooperation and Development (OECD) in 1980,[49] and became the basis for many privacy laws and policies around the world.

Eventually, FIPs faded into the background, not because the policies were wrong, but because the general policies that served so well for so long were not specific enough to address ongoing developments in technology, industry, and government. To offer one example, FIPs did not call for privacy agencies, but countries quickly recognized the value of privacy agencies or data protection authorities, and the idea spread around the world. Data protection authorities function as enforcers of data protection and governance laws, and they help guide the implementation data governance ecosystems at the ground level effectively.[50]

Countries enacted different privacy laws beginning in the 1970s and 1980s. It did not take long before the differences and limits in these national laws created problems with international data flows. Europe begin to address these problems, and the EU, after some significant effort, adopted a Data Protection Directive in the 1990s.[51] The shortcomings of the Directive and the challenges with its implementation resulted in

articulated in the Maori approach, among others. In these cases, as discussed in this paper, privacy is seen as a community feature belonging to a group of people. See First Nations Information Governance Centre, *The First Nations Principles of OCAP,* https://fnigc.ca/ocap-training/(establishes how First Nations' data and information will be collected, protected, used, or shared); see also Te Mana Raraunga, the Māori Data Sovereignty Network, https://www.temanararaunga.maori.nz . For a general discussion of privacy, See Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the books and on the ground,* 63 Stanford Law Review 247 (2011) (UC Berkeley Public Law Research Paper No. 1568385), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385> [12.11.2025].

[47] The state of Hesse, Germany passed a federal law that regulated automated data processing in the public sector on October 7, 1970. (Bundesdatenschutzgesetz, or BDSG). In the same month and year, the U.S. passed its first major privacy law, the Fair Credit Reporting Act, which also is among the first laws to regulate machine learning. Other laws followed in the EU and the U.S. In 1981, the EU opened its Convention 108 for signature by EU members, and also by other countries. In the 1990s, the EU passed its landmark data protection Council Directive EU 95/46. More than 160 jurisdictions across the world now have some form of data governance/data protection legislation, mostly following the pattern of the second generation of EU 95/46, the EU General Data Protection Regulation. The uptake of the GDPR comprises a mature and nearly global regulatory footprint although significant differences in policy and implementation remain.

[48] *Gellman R.,* Fair Information Practices: A Basic History, Version 2.32 (July 2025), <https://bobgellman.com/rg-docs/rg-FIPShistory.pdf> [12.11.2025].

[49] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Feb. 12, 2002), <https://doi.org/10.1787/9789264196391-en> [12.11.2025].

[50] See generally Global Privacy Assembly, https://globalprivacyassembly.org, (the Assembly is comprised of the international data protection and privacy commissioners or authorities. They met the first time in 1979). See also Irish Data Protection Commission, https://www.dataprotection.ie; Data Protection Office Mauritius, https://dataprotection.govmu.org/SitePages/Index.aspx; Personal Information Protection Commission Japan, https://www.ppc.go.jp/en/; Office of the Privacy Commissioner for New Zealand (Te Mana Matapono Matatapu), <https://www.privacy.org.nz/privacy-act-2020/privacy-principles> [12.11.2025] (examples of the work of data protection authorities).

[51] Directive 95/46/EC, 1995 O.J. (L 281) 31.

its replacement by the EU General Data Protection Regulation[52] which has been enforced since 2018. Many other countries around the world now follow the EU privacy model in some manner.[53] There is little to no question that GDPR is normative. The GDPR forms the foundation for a nearly global set of data protection laws today.[54]

However, as privacy laws and institutions spread into the developing world, it became clear over time that solutions that seemed responsive in theory did not always work well in practice. Sometimes, ideas that worked in one context or jurisdiction or social context did not fit in others.[55] For example, GDPR-like legislation, with its focus on individual privacy rights does not always fit well in indigenous contexts, where privacy and data are often handled as community rights.[56] GDPR-like legislation has also been a difficult task for small island nations, who often have very small populations and may not have enough resources to launch a comprehensive data protection regime.[57] The data governance and privacy learning curve stretches over decades, and the various stakeholders in the data ecosystems are still learning.

A significant global conversation is underway in the data protection sphere regarding the relationship between the GDPR and AI. Among the many questions at

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[53] Pam Dixon, research; John Emerson, data visualization and design, *Global Table of Countries with Data Privacy Laws, Treaties, or Conventions*, World Privacy Forum, June 2024, <https://worldprivacyforum.org/posts/countries-with-data-privacy-laws/> [12.11.2025].

[54] More than 165 countries or jurisdictions have passed either GDPR, or very similar legislation, or have a draft bill. See Dixon and Emerson, *Global Table of Countries with Data Privacy Laws, Treaties, or Conventions*, World Privacy Forum. For a detailed discussion of GDPR and its impact, See: Graham Greenleaf, *Global Data Privacy Laws 2023: International Standards Stall, but UK Disrupts,* Privacy Laws & Business International Report 8-15, UNSW Law Research Paper No. 23-50, (2023). See also: Graham Greenleaf, *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills.* Privacy Laws and Business International Report (PLBIR) 1, 2-4, UNSW Law Research Paper No. 23-48, February 2023.

[55] Michael Pisa, Pam Dixon, Benno Ndulu, Ugonma Nwankwo, *Governing Data for Development: Trends, Challenges, and Opportunities,* Center for Global Development, November 12, 2020. https://www.cgdev.org/publication/governing-data-development-trends-challenges-and-opportunities.

[56] As discussed in this paper, there have been significant advances in regards to the data rights of Indigenous people. This extends to the rights of Indigenous people to develop their own methods of data governance, which can, depending on context, grant community-level privacy rights which operate substantially differently than individual privacy rights enshrined in the GDPR. These contextual differences have meaningful implications for AI governance tools and their use. See First Nations Information Governance Centre, *The First Nations Principles of OCAP*, https://fnigc.ca/ocap-training/(establishes how First Nations' data and information will be collected, protected, used, or shared); see also Te Mana Raraunga, the Māori Data Sovereignty Network, https://www.temanararaunga.maori.nz; see also United Nations, G.A. Res 61/295 art. 18 (Sept. 13, 2007) (provides Indigenous peoples' right to participate in decision-making in matters which would affect their rights, through representatives chosen by them in accordance with their own procedures, as well as to maintain and develop their own Indigenous decision-making institutions).

[57] Pam Dixon, research; John Emerson, data visualization and design, *Global Table of Countries with Data Privacy Laws, Treaties, or Conventions*, World Privacy Forum, June 2024. https://worldprivacyforum.org/posts/countries-with-data-privacy-laws/ . See in particular: Small Island Nations filter. The small island group of countries has notably low adoption of GDPR-like regulations.

hand are those interrogating whether the GDPR is fit for purpose regarding AI privacy challenges, or whether there should be new privacy regulations that focus only on AI or its subset issues such as generative forms of AI.

The pace of regulatory activity addressing AI contrasts with the development of data governance and privacy laws and norms, which took place over a long period of time. Certain advanced forms of AI, however, jumped to public and policy awareness quite rapidly in comparison to the pace of privacy regulatory activity. One example may be seen in the days and months following the launch of ChatGPT in November 2022.[58] ChatGPT and generative AI models captured the interest of many regulators. Discussions, proposals, and rules of varying quality for generative AI models resulted, and rapidly so.[59]

To date, the initial flurry of activity has resulted in the fairly rapid passage of many focused laws at the subnational level, for example, many jurisdictions have passed narrow legislation regarding generative AI, among other narrower topics addressing AI issues.[60]

The European Union's AI Act is the most significant comprehensive AI bill to be enacted thus far.[61] While most countries have not yet followed Europe's example yet, there is a great deal of activity and discussion around AI-related legislation and a great deal of discussion around individual privacy rights in the AI context.[62] It is worth recalling that various forms of machine learning have been used and regulated for many decades. Credit score regulations —addressing data inputs, algorithms, set points, and other aspects of machine learning — exist in some jurisdictions and have since the 1970s.[63] These early forms of machine learning regulations often include well-understood and familiar governance mechanisms, such as error correction, a formal dispute process, government oversight, and other forms of consumer redress. These established methods of governance of credit scoring are well-understood. The procedural, and administrative controls used in these types of regulations are international norms. But today these normative solutions to privacy challenges are not as effective within certain AI contexts. The new territory of advanced AI is much more

[58] *Introducing ChatGPT*, OpenAI, 30 November 2022, <https://openai.com/index/chatgpt/> [12.11.2025].
[59] See generally the OECD AI Observatory, particularly the *Global AI law and Policy Tracker,* AI Observatory, OECD, <https://oecd.ai/en/dashboards/policy-initiatives> [12.11.2025].
[60] In the U.S. as of 2025 all 50 states have introduced or enacted laws regarding AI. See National Conference of State Legislators, *Artificial Intelligence Legislation Tracker*. <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation> [12.11.2025].
[61] EU Artificial Intelligence Act, Regulation – EU – 2024/1689. As mentioned in note 29, this paper does not analyze the EU AI Act's impact on collective privacy; while the EU AI Act does discuss groups in several specific contexts, for example, it prohibits discrimination in credit scoring, the discussion in the Act is not focused on privacy. The EU AI Act does not specifically address privacy, so it is not analyzed here as the focus is on collective privacy.
[62] *OECD AI Policy Navigator*, AI Observatory, OECD, <https://oecd.ai/en/dashboards/national> [12.11.2025]. See also: IAPP Global AI Law and Policy Tracker, IAPP. <https://iapp.org/resources/article/global-ai-legislation-tracker/> [12.11.2025].
[63] The Fair Credit Reporting Act in the U.S. is an exemplar of such a regulation. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.

uncharted, particularly in regards to how privacy itself is changing within AI ecosystems.[64]

One of the questions raised by the advances in AI is if the established methods of governance currently used in individual rights-based privacy-focused regulations and policies are going to be sufficient to address collective forms of privacy risks that are emerging, particularly in AI and machine learning ecosystems. Not all of the answers are fully developed yet, but it is becoming clearer that collective privacy is emergent as a new area that will need to be addressed. The case studies in this paper shine a light as to where key gaps are in the current system of privacy governance and raise key questions about how to begin thinking about this area of risk more systematically.

5. Case Studies in Collective Privacy

This paper examines three distinct case studies in collective privacy. The case studies were selected because the groups involved exhibit demonstrable entitativity, which is necessary to find case studies that are clear enough for an analysis.

The first case study focuses on indigenous collective data privacy rights, first broadly, then with a focus on the government treaty that establishes collective privacy for the Maori. This is a highly defined, high entitativity group, and the case study is focused on and legislatively defines collective privacy with specificity. The second case study is focused collective privacy and the biomedical analysis of genetic data, which includes another high entitativity group, that of the analysis of Native Americans' DNA in the context of a large U.S. genetic biobank. In this case study, there is an exceptional discussion of consent in the context of collective privacy and the failure of existing law to be able to protect the genetic data from reidentification. The third case study is of a holocaust survivor who was defamed as part of a collective group of survivors of the Mauthausen concentration camp; he sued on the basis that although the defamation was collective, that the privacy rights afforded to him by law should still apply because he was an identifiable member of the collective group. This case was heard before the European Court of Justice and was decided in his favor.

[64] A global review of AI governance tools and analysis of their effectiveness and fitness for purpose concluded that current privacy norms do not yet address the full range of the forthcoming problems related to privacy automation -- essentially machine oversight at scale – among other challenges. Kate Kaye and Pam Dixon, *Risky Analysis: Assessing and Improving AI Governance Tools - An International review of AI governance tools and suggestions for pathways forward*, World Privacy Forum, December 2023.

5.1. Case Study: Indigenous Collective Privacy Rights and Data Sovereignty

While most legislation today principally articulates privacy and related rights as individual rights, privacy also exists as a collective or community-based privacy right as well.[65] Group privacy can be found throughout the governance spectrum, from multilateral to national to tribal.

International Customary Law[66] provides significant indigenous rights to privacy and data sovereignty. The most important document is the United Nations Declaration on the Rights of Indigenous Peoples, (UNDRIP), which sets forth core rights of indigenous peoples to govern themselves.[67] Several governments also apply the same principles to AI governance.

Several articles of UNDRIP outline the key contours of collective rights, autonomy, self-government, and certain rights to privacy, among others:

> Article 4
>
> Indigenous peoples, in exercising their right to self-determination, have the right to autonomy or self-government in matters relating to their internal and local affairs, as well as ways and means for financing their autonomous functions.
>
> Article 7
>
> 1. Indigenous individuals have the rights to life, physical and mental integrity, liberty and security of person.
>
> 2. Indigenous peoples have the collective right to live in freedom, peace and security as distinct peoples and shall not be subjected to any act of genocide or any other act of violence, including forcibly removing children of the group to another group.
>
> Article 12

[65] For example, the Māori have distinct and well-developed concepts of collective privacy enshrined in their culture as well as tribal laws. The Māori consider privacy to be a collective right, to be effectuated collectively. There is a detailed and nuanced literature around concept of collective privacy for the Māori. This paper introduces the concept and develops it in contrast to individual concepts of privacy. However, for a detailed articulation of what indigenous peoples consider to be collective privacy, the original source material is essential to study. See, e.g., Khylee Quince and Jayden Houghton, *Privacy and Māori Concepts* in Stephen Penk and Nikki Chamberlain (eds) _Privacy Law in New Zealand_ (3rd ed, Thomson Reuters, Wellington, 2023) 43–136.

[66] Customary international law refers to international obligations arising from established international practices and not from formal written conventions and treaties. International Customary Law relevant to indigenous rights and privacy includes the United Nations Declaration on the Rights of Indigenous Peoples, (UNDRIP), which sets forth core rights of indigenous peoples to govern themselves. In national legislation, these ideas are set out in for example, the U.S. Federal Indian Law, Canadian law, and New Zealand law, among others.

[67] United Nations Declaration on the Rights of Indigenous Peoples, Resolution adopted by the General Assembly on 13 September 2007, 62/295.

1. Indigenous peoples have the right to manifest, practise, develop and teach their spiritual and religious traditions, customs and ceremonies; the right to maintain, protect, and have access in privacy to their religious and cultural sites; the right to the use and control of their ceremonial objects; and the right to the repatriation of their human remains.

Article 18

Indigenous peoples have the right to participate in decision-making in matters which would affect their rights, through representatives chosen by themselves in accordance with their own procedures, as well as to maintain and develop their own indigenous decision-making institutions.

Article 19

States shall consult and cooperate in good faith with the indigenous peoples concerned through their own representative institutions in order to obtain their free, prior and informed consent before adopting and implementing legislative or ad ministrative measures that may affect them.

In national legislation, these ideas are set out in U.S. Federal Indian Law, Canadian law, and New Zealand law, among others. Further, important policy literature written by indigenous people's addresses data held at the tribal level. Tsosie, a major contributor to this literature, argues that tribal governments possess the authority to enact data privacy laws at the tribal level to define what constitutes "tribal data." [68] This is a foundational issue that is highly relevant to AI and research, among other areas. Related issues are collective data ownership, collective privacy rights, and the collective application of ethical principles. These types of approaches can be seen, for example, in the U.S. Indigenous Data Sovereignty Network and the Māori Data Governance Model, Te Kāhui Raraunga. Another indigenous governance framework is the First Nations Principles of OCAP.[69] OCAP, (Ownership, Control, Access, and Possession) expressly establishes how First Nations' data and information in Canada will be collected, protected, used, or shared. Any AI standards development work in Canada should ensure that the OCAP principles are respected and that representatives from Canada's First Nations can participate in the standards development processes.

[68] *Tsosie R.,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019)

[69] *The First Nations Principles of OCAP*, First Nations Information Governance Centre, <https://fnigc.ca/ocap-training/> [12.11.2025].

In regards to AI specifically, the Māori crafted an important and influential policy literature, in which Kukutai et al explain that indigenous concepts of privacy are inherently collective. The New Zealand government works with the Maori to co-develop AI policy frameworks to be used whenever indigenous data or rights may be involved. New Zealand's approach to AI sets an important precedent. The structure of New Zealand's approach is set to make a potentially significant long term impact on global standardization models and efforts.

5.2. New Zealand Government's and the Māori's Data Governance Co-design Efforts

First, by way of background, New Zealand started early in its work on AI. In 2017, it established a Government Chief Data Steward (GCDS) role via mandate. New Zealand already has a body of work and practice regarding data stewardship.[70] The Chief Data Steward is role is filled by the Chief Executive of Statistics New Zealand (Stats New Zealand). The role has several functions: to set mandatory standards; to enable a "common approach to the collection, management and use of data across government;" and to "direct the adoption of common data capabilities."

The Chief Data Steward developed a Data Strategy and Roadmap,[71] provided leadership in developing transparency and accountability for AI in the government context,[72] created a broad Data Stewardship Framework, ~~work on open data,~~ and developed a cooperative framework collaboratively with the Māori.[73] This effort initially sought to ensure that work done regarding Covid-19 was respectful to Maori approaches. Subsequently, this work was extended further in AI and into and accountability and standards development processes in collaboration with the Maori.

Structurally, New Zealand's framework of data stewardship is inclusive and interdependent across the whole of government. New Zealand describes its data stewardship framework as including a range of roles with governance functions in New Zealand's data system, including the:

---

[70] Government Chief Data Steward Mandate, Office of the Minister of Statistics New Zealand, <https://www.stats.govt.nz/assets/Uploads/Corporate/Cabinet-papers/Strengthening-data-leadership-across-government-to-enable-more-effective-public-services/strengthening-data-leadership-across-government-to-enable-more-effective-public-services-redacted.pdf> [12.11.2025].

[71] *The Government Data Strategy and Roadmap*, Government Chief Data Steward, September 2021, <https://www.data.govt.nz/leadership/strategy-and-roadmap/> [12.11.2025].

[72] Algorithm Assessment Report, Stats NZ, 2018, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-assessment-report/> [12.11.2025].

[73] Māori Data Governance Co-design Review, Te Kāhui Raraunga, January 2021, <https://www.kahuiraraunga.io/_files/ugd/b8e45c_0b1a378da21c459eb4fb88dfbf6aea81.pdf> [12.11.2025]. See also: COVID-19 Lessons Learnt: recommendations for improving the resilience of New Zealand's government data system. Stats NZ Tatauranga Aotearoa, March 2021, <https://data.govt.nz/docs/covid-19-recs-report/> [12.11.2025].

- Government Chief Data Steward,
- Government Chief Information Security Officer,
- Government Chief Digital Officer,
- Government Chief Privacy Officer,

The Privacy Commissioner, Ombudsman, Auditor General, and Chief Archivist also have roles.

The Privacy Commissioner's role is defined in the NZ Privacy Act of 2020, which has 13 information privacy principles, and requires agencies to report certain data breaches to the Privacy Commissioner. New Zealand's privacy laws are aware of GDPR, and as such it qualifies as a modern data protection law, but the Act is not identical to GDPR and uses different terminology.

New Zealand's approach to algorithms, or AI and machine learning is progressive and inclusive. In 2018, New Zealand released its Algorithm Assessment report, which covered the practices of 14 government agencies.[74] It is among the earliest instances of a robust, mature discussion of data governance, management, standards, stewardship, open data, and privacy in the area of government use of algorithms. The 2018 report led to the July 2020 release of the first iteration of the Algorithm Charter for Aotearoa New Zealand by the Minister of Statistics.[75] The Charter is notable for its approach to providing for means of appeal of decisions informed by AI. New Zealand also released an initial algorithm toolkit in 2021 to implement the charter.[76]

As of 2024, the government of New Zealand has updated and expanded its AI-related materials in regards to its charter in an overarching toolkit, with its most recent update being 2023.[77] There are many features of the toolkit that are worth imitating, including the impressive list of signatories to the charter. These signatories specifically include the Ministry of Māori Development as well as other NZ Ministries.

Specific to indigenous-informed approaches to AI is the New Zealand Government's Algorithm impact assessment user guide.[78] The Guide offers a detailed discussion of New Zealand's relationship with the Māori. It reflects with specificity its commitment to honor the Māori approach to data and ensures the use of algorithms is consistent with the articles and provisions in its charter.

[74] Algorithm Assessment Report, Stats NZ, 2018, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-assessment-report/> [12.11.2025].

[75] Algorithm Charter for Aotearoa New Zealand, Stats NZ. July 2020, <https://www.data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf> [12.11.2025].

[76] Government Algorithm Transparency and Accountability, Stats NZ. March 2021, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability> [12.11.2025].

[77] Algorithm Charter for Aotearoa New Zealand, which includes foundational work from the following: Principles for the safe and effective use of data and analytics Government use of artificial intelligence in New Zealand. Trustworthy AI in Aotearoa - AI principles Open government partnership Data protection and use policy and Privacy, human rights, and ethics framework.

[78] Algorithm impact assessment user guide, New Zealand Government, Te Kāwanatanga o Aotearoa, December 2023, <https://data.govt.nz/assets/data-ethics/algorithm/AIA-user-guide.pdf> [12.11.2025].

The guide notes on p. 29:

"General guidance to meet the Partnership commitment in the Charter you should:

- incorporate te ao Mãori perspectives into the design and use of algorithms
- ensure algorithm development and use is consistent with Te Tiriti o Waitangi
- consider how Mäori data sovereignty will be maintained
- assess how algorithm use will impact iwi and Mäori.

Te ao Mäori acknowledges the interconnectedness and interrelationship of all living and non-living things via spiritual, cognitive, and physical lenses. This holistic approach seeks to understand the whole environment, not just parts of it. (This definition comes from Treaty of Waitangi/Te Tiriti and Mãori Ethics Guidelines for: Al, Algorithms, Data and IOT.)"

Further into the Algorithmic assessment user guide, Question 5.3 on page 32 notes that:

"Mãori data is not owned by any one individual, but is owned collectively by one or more whanau, hapu or iwi. Individuals' rights (including privacy rights), risks and benefits in relation to data need to be balanced with those of the groups of which they are a part. (This definition comes from https://www.temanararaunga.maori.nz/)
Mäori data sovereignty recognises that Mäori data should be subject to Mãori governance — the right of Mäori to own, control, access and possess Mãori data. Mãori data sovereignty supports tribal sovereignty and the realisation of Mäori and iwi aspirations. (This definition comes from https: // www.temanararaunga.maori.nz/)"

The express acknowledgement of indigenous approaches to data and AI by the government of New Zealand in its AI policy sets a critically important example for other governments to follow. It is possible to incorporate multiple points of view regarding data. It will be important to ensure that global standards development efforts take note of the indigenous approaches that are either formal guidance or law in other countries. Arguably, standards efforts would do well to look into informal guidance as well.

For AI standards and policy in the indigenous context, several national governments adopted UNDRIP as a matter of national law. For example, New Zealand is a signatory to UNDRIP and has formal agreements. In 2021, Canada passed an Act

respecting the United Nations Declaration on the Rights of Indigenous Peoples [79] This bill brings Canadian law into alignment with UNDRIP.

5.3. Case Study: Human Subject Biomedical Research and Collective Privacy: "Broad Consent" to Research Uses of Genetic Biobank Data May Not Covered Under the Common Rule or Other Health or Research Privacy Law

Human subjects of biomedical research may often have collective privacy interests in biobanks holding their biological or genetic samples and other data that is used in the aggregate for analysis in medical research. An important case study in this realm comes from a large biomedical research effort in the U.S. In 2015, the National Institutes of Health (NIH) in the United States launched a precision medicine initiative that sought to collect 1 million biospecimens for study.[80] [81] The NIH consulted with tribal stakeholders for its biobank project, and has publicly acknowledged tribal sovereignty. The NIH wrote a report about this engagement in 2023 [82] The report is groundbreaking in many ways, and contains an important articulation of tribal concerns. According to the report, "Through the consultation process, tribal leaders have expressed deep concern about the use of data for secondary (future) research…"[83]

Also in the report, the NIH specifically described group or collective privacy impacts, which in this case could stem from the ability to identify a tribal research participant as part of an identifiable group.

The NIH's response to this concern is important because it contains a rare discussion of the idea of "broad consent" and the secondary use of the data identified as belonging to a particular group in the context of deidentification. Deidentification, in the U.S. context, as discussed in this paper, typically creates exemptions from privacy law, even when genetic or biological data is involved, depending on the context. This exemption is particularly difficult when it applies to research that includes biological samples and the potential for genetic linking. This is a deeply nuanced and difficult area of policy.

[79] An Act respecting the United Nations Declaration on the Rights of Indigenous Peoples, Bill C-15, Parliament of Canada, <https://www.parl.ca/LegisInfo/en/bill/43-2/C-15> [12.11.2025].
[80] *All of Us Research Program,* National Institutes of Health, <https://allofus.nih.gov/about/faq> [12.11.2025].
[81] Gellman R., Dixon P., Privacy, the Precision Medicine Initiative, & the All of Us Research Program: Will Any Legal Protections Apply? World Privacy Forum, March 16, 2017.
[82] All of Us Tribal Engagement, NIH, <https://allofus.nih.gov/about/diversity-and-inclusion/tribal-engagement> [12.11.2025].
[83] *All of Us Research Program Tribal Consultation Final Report March 2021*, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].

The NIH stated in its report:

"Broad consent and secondary research

All data and biospecimens provided through the research platform will be de-identified in compliance with the standards of the Common Rule, and All of Us does not plan to share any readily identifiable data or biospecimens. All of Us currently does not seek broad consent for secondary research as defined in the 2018 Common Rule. That type of broad consent is required only when the secondary use will consist of readily identifiable data and samples. Data types are deemed "identifiable" if there is a significant chance that the data, either alone or in combination with other data, would render the identitativity of an individual participant readily discoverable. In other words, identifiability is less about an individual data element than about the data in context. Nevertheless, certain information, such as a name or Social Security number, would be inherently identifiable. In addition, certain other data elements, such as narrative fields from electronic health records, where such identifiers are more likely to be featured, are deemed potentially identifiable and must be heavily altered before becoming eligible to be shared with researchers.

The discussion of identifiability at the individual level, however, does not take into consideration the concern over group identifiability. In most cases, creating definable groups within data is a crucial part of the research process. In some cases, allowing for subpopulations to be singled out can put these subpopulations at risk for stigma and discrimination. The All of Us Research Program actively works to prevent, to the extent possible, the conduct of any stigmatizing or discriminatory research with the All of Us resources. The program also acknowledges that some groups, communities, and other defined subpopulations, even where stigma or discrimination may be a risk, may wish to make their group, community, or subpopulation discoverable within the dataset in the interests of promoting research that could address health disparities. However, particularly where there are historical reasons contributing to elevated risk of stigmatizing or discriminatory research, All of Us will look for guidance from those groups, communities, and subpopulations, including Tribal Nations, for how to approach group identifiability and appropriate harm mitigation strategies.

The program recognizes that there is a concept of broad consent that is not fully accounted for by broad consent as defined by regulation. The program acknowledges that it is requesting broad consent from participants according to the conceptual interpretation, rather than the specific regulatory provision in the 2018 Common Rule." [84] [Emphasis supplied].

Among the privacy challenges in human subject research in large biobank contexts is that existing privacy protections that depend on the use of deidentification as a privacy-preserving tool do not always apply. Genetic identification of groups of

[84] *All of Us Research Program Tribal Consultation Final Report* March 2021, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].

people is possible within deidentified datasets, depending on context. In the NIH study, the NIH admits that there is a risk of identifiability of biospecimens to a broader and identifiable group, and it acknowledges that existing Common Rule protections do not address this risk. This is noted in the statement: "The program acknowledges that it is requesting broad consent from participants according to the conceptual interpretation, rather than the specific regulatory provision in the 2018 Common Rule." [85] Broad consent, again, is particularly challenging policy issue, and it is essential to resolve the question of what to do with "broad consent" in the tribal context, as well as outside of the tribal context.

In addition to this risk, an additional challenge, is that the right to collective privacy will make it very challenging to protect in an environment saturated with AI processing of biobank data samples. These two trends interact with each so as to deeply exacerbate the challenges for effectuating either individual or collective privacy in certain biobank contexts. The NIH's use of the term "identitativity" to describe the risk biospecimens may have regarding identifiability to a particular group is helpful here, as it interacts with the literature on entitativity, particularly as seen in the Lewit case study which follows.

5.4. Case Study: Lewit v. Austria and the European Court of Human Rights Regarding Individual Members of Collective Groups

In July 2016, Mr. Aba Lewit of Austria filed an appeal of a claim for compensation related to a defamation case to the European Court of Human Rights,[86] alleging that his privacy rights had been violated when a group of concentration camp survivors that he was part of were collectively defamed by a right wing publication. The case was unusual in that the publication in question did not specifically name Lewit or any of the other former prisoners, rather, the publication named as a collective group the survivors who had been liberated from the Mauthausen concentration camp in 1945. The publication had described the concentration camp survivors in highly derogatory terms, including characterizing them as having participated in criminal activities.

Initially, in June 2016, a group of 8 former Mauthausen camp prisoners plus 2 others, a daughter of a deceased former Mauthausen prisoner and a former prisoner at the Theresienstadt concentration camp, brought a defamation case before the Graz Civil Court. The Graz Civil Court granted an interim injunction in August of that same year, which was upheld on appeal and also upheld by the Supreme Court. In February 2017 the proceedings were terminated by a court settlement which required the

[85] *All of Us Research Program Tribal Consultation Final Report* March 2021, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].
[86] *Lewit v. Austria*, Application No. 4782 / 18, Judgment 10 October 2019).

publication to issue a retraction. Because Lewit was not a party to the June 2016 claim, he was not bound by this settlement.

In a separate proceeding, 9 of the 10 claimants from the initial defamation suit plus Lewitt filed for compensatory damages resulting from the defamatory article. The ECHR described the arguments the group of survivors made regarding their identitativity, or potential for identification as a member of a specific group, as follows:

"The claimants argued that in defamation cases against a group of people, it was decisive for the question of their legal standing that every individual belonging to that group was identifiable, even if not named personally - which was the case here. They reiterated that they had all been victims of the National Socialist regime, and had been imprisoned because of their origins, their beliefs or their faith. At the time of their arrest and/or deportation to the concentration camps, some of them had been children, and others political detainees. They had never committed any criminally significant acts, either before their imprisonment or after their liberation from the concentration camps."[87]

Despite these arguments, in September 2016, the Graz Regional Criminal Court dismissed the survivors' claims for compensation. The ECHR discussion of this fact noted that "…The decisive question for the court was whether an average consumer would individually recognize the claimants and would associate the defamatory allegations with them" (Para 21). The Criminal Court's specific argument was premised on the fact that in 1945 there were around 20,000 survivors who had been liberated from the camp, which in its judgment was too large of a collective group to allow for the identification of individual member of that group. The Austrian lower court essentially used an argument of privacy through numerical obscurity to deny standing to the individual members of the collective group.

It was Lewit who made an appeal of the Austrian court's decision to the Grand Court. In the appeal, Lewit argued that the suit was wrongfully decided, and that he was in fact identifiable because at the time, he was 96 years old and was one of only a very few survivors of Mauthausen still alive. As such, at the time of the article's publication he was identifiable by members of the local community as a Mauthausen survivor and thus was defamed by the publication's remarks about the group. The ECHR discussed this issue in its decision that: "The Court has held that any negative stereotyping of a group, when it reaches a certain level, is capable of impacting on the group's sense of identity and the feelings of self-worth and self-confidence of members of the group. It is in this sense that it can be seen as affecting the private life of members of the group (see Aksu v. Turkey [GC], nos. 4149/04 and 41029/04, § 58, ECHR 2012). The Court considers that similar considerations apply in the instant case, when it comes to the defamation of former Mauthausen prisoners, who, as survivors of the Holocaust, can be seen as constituting a (heterogeneous) social group." (Para. 46)

The ECHR also noted that in cases where groups were seeking damages for defamation that… "If the group consists of a large number of people, the domestic courts have generally found that individuals were not affected. However, in certain

[87] Id. At Paragraph 19.

cases the Supreme Court has accepted that members of larger groups were personally affected (see for instance judgments of 11 January 1978, no. 10 OS 196/77 and 29 June 2011, no. 15 OS 15q/10k.) (Para. 36).

The ECHR ultimately agreed with Lewit, and convicted the Republic of Austria for violating Article 8 of the European Convention on Human Rights, which protects private and family life. The court found that the lower Austrian courts had wrongfully dismissed the original defamation lawsuits brought by the Mauthausen survivors, and that the corresponding judgments were seriously flawed in their reasoning. The ECHR ruled that the lower courts should have properly evaluated the number of remaining survivors of the Mauthausen concentration camp in 2016, and whether the survivors could be individually identifiable.

The ECHR's judgment is now used in training activities for judges and candidate judges in order to increase sensitivity for cases with references to Austria's past. Abe Lewit died in November 2020 at the age of 97. He lived to see his case successfully decided in his favor.

This case study brings forward several critically important issues in considering collective privacy. Certainly a core issue is that the camp survivors in this case had to prove individual identifiability or impact at an individual level to be able to effectuate their privacy rights under European law. This was made very clear throughout the case. It was only in proving individual identifiability and impact that Lewit was able to successfully bring his case.

The Levit case further sharpens the question that was raised in the biomedical case study in this paper: that is, what is the risk that an individual has of being reidentified back to a particular group? How does this risk change with the entitativity of a particular group? Are there factors that increase or decrease the risk? This paper postulates that if there is a history of stigma or discriminatory actions against a definable group with high entitativity, then a potential for identitivity to that group can represent a risk in and of itself. This postulation raises many additional questions.

It is arguable that even at a high number like 20,000, that the Mauthausen survivor group had many pathways of vulnerability regarding identification to Mathausen and potential stigma. Hiding in a big crowd is not effective "privacy by obscurity" in every case. This was true for the Mauthausen survivors in their lifetimes, and it is also true for those living in a digitalized world. So, when should group privacy be defensible under privacy law? Only when the group is small? Only when there is the possibility of identification with the group?

The NIH in its report discussed identitativity as the test for potential stigma. If a test for the risk of identitativty of an individual back to a group to determine privacy risk can be taken as a hypothesis, then it is the identitativity created by the contextual relationship of an individual to a group that matters, and this may not be dependent on group size. Identitativity may occur in groups of many sizes. No matter what the questions may be, one thing is certain: Lewit was forced to prove his *identifiability* to

a group that had characteristics of high sparsity in order to effectuate his privacy rights.

While the Lewit case was properly decided given its parameters, it does highlight a meaningful gap in privacy protections; in a digitalized world, high-sparsity (or low numbers of group members) should not be the gauge by which a right to privacy is determined; this is because a potentially stigmatizing analysis that identifies group members can be accomplished at scale and quickly in today's digital ecosystems. The larger group of Mathausen survivors from 1945 onward may have had experiences of stigma even with the higher numbers of group members.

Regarding entitativity, two of the exemplars in this paper describe groups with high entitativity based on significant ethnic and tribal linkages. In the Lewit case, the group demonstrated high entitativity in that the group were bounded by their shared history as prisoners of the notorious Mauthausen concentration camp,[88] and then lived for many years to interact as survivors of that ordeal. The research on entitativity indicates that there are different types of entitativity, and groups can arrive at entitativity in different ways. The Mulhausen concentration camp imprisoned people from multiple ethnic backgrounds, including people of Romani origin, among others.[89] This leads to the reasoning that the uniqueness of the collective group of survivors, and their historic significance are among the key qualities of the group's entitativity. Without being able to interview the survivors, it is difficult to determine definitively what additional qualities may have added to the entitativity.

In 2016, when very few individuals were left of the original group, a question arises as to how the entitativity of this group may have changed over time. How did sparsity impact the entitativity of the group? Was the shared experienced of both a traumatic and historic nature the core of the entitativity of this group?

6. Conclusion

Today, the strongest protections in collective privacy includes those for tribal groups that have certain rights under UNDRIP, and may also have additional rights based on further laws, treaties, or agreements. The Māori, as discussed extensively in this analysis, have formal collective privacy rights through an agreement with the government of New Zealand. The NIH All of Us report identified something quite important, that even non-identifiable individuals, if they are able to be connected to a larger group with entitativity, may suffer from certain stigmas or discriminations by that associativeness.

Under the normative privacy thought that is enshrined in the majority of country-level privacy legislation today, it is primarily individuals who are granted certain privacy rights. As was well-stated and proven in the NIH report, "The discussion of

[88] *76 years later, we remember Simon Wiesenthal's liberation from Mauthausen*, Simon Wiesenthal Center, 6 May 2021, <https://www.wiesenthal.com/about/news/76-years-later-we-remember.html> [12.11.2025].
[89] Mauthausen Concentration Camp, Wikipedia, <https://en.wikipedia.org/wiki/Mauthausen_concentration_camp> [12.11.2025].

identifiability at the individual level, however, does not take into consideration the concern over group identifiability." The Lewit case before the European Court of Human Rights was decided in his favor because he could prove his identifiability as an individual and therefore was able to effectuate the rights afforded to him individually under the European Charter of Human Rights. The collective group of survivors of the notorious Mauthausen concentration camp did not qualify under the law at that time for collective privacy protections. The European Court of Human Rights did rule in Lewit's favor, and it wrestled in its decision with the conflict between individual rights of privacy and that in some situations group-related privacy harms may affect individuals.

The individual focus on current normative privacy law has been functional for many years and is useful. But an ocean of digitalized information and data about people and groups of people is now interacting with advanced versions of AI and machine learning which have capabilities to create groups, make inferences about groups, and apply these inferences, in some cases with particularity, rapidly, and at scale. AI is becoming an increasing part and parcel of many aspects of modern life. It is important to look at groups of people, and specifically at the issue of collective privacy and think broadly and widely about what privacy protections may be needed for groups, in what circumstances, and what that process might be.

There are significant questions that need to be asked and addressed in the context of collective privacy. Among the first of these questions is how can a group be meaningfully identified as rising to the level of needing collective privacy protections or rights? The concept of entitativity is helpful here, but more work is needed to respond to the question of what the NIH report terms "group identitativity." This is a term that is not used frequently in discussing privacy, but the NIH and Lewit case studies indicate that the issue of group identitativity needs to be discussed.

When does being part of a group – or being identifiable to a particular group - rise to importance regarding collective privacy needs? When, specifically, and in what contexts do collective privacy rights matter? This is hopefully a conversation that will be undertaken by as many stakeholders as possible and inclusive of the indigenous, technical, policy, legal, human rights, privacy, and other experts needed for providing inputs and analysis.

In looking for existing frameworks that might be used to address the challenging issues regarding group privacy, the history of indigenous peoples' and the longstanding, detailed governance philosophy and frameworks that exists around collective privacy is arguably among the most, if not the most, instructive and important governance that is already in place. The Māori approaches in New Zealand stand as important and specific exemplars of respectful and workable approaches, and the treaty that exists between New Zealand and the Māori provides precise language that can be studied in the collective privacy context.

The biobank context is an extremely challenging one. What protections will be needed as biomedical analysis becomes more and more capable? The tribal collective privacy gaps regarding broad consent have already been documented. Are there challenges for additional groups? Can these challenges be quantified so as to create solutions?

There are many lessons that can be drawn from what is now known about collective privacy. Lessons can be drawn regarding collective privacy from socio-technical challenges and approaches to solutions in the AI context, and there are also critical lessons to be learned in certain types of human subject research, particularly in biobanks. Fortunately, exemplars of existing policies in collective privacy in the indigenous context can provide a starting point.

The issue of collective privacy deserves substantial attention and research going forward, including assessing and addressing collective privacy risks from AI analysis and applications, and including learning from indigenous frameworks that are already in place. To leave this work undone would be to miss an opportunity to address a meaningful technical and philosophical shift that is developing in our time. The opportunity to address collective privacy risks and solve the problems these risks can present is one that must not be squandered.

Bibliography:

1. Declaration on the Rights of Indigenous Peoples, United Nations, (adopted 2 October 2007 UNGA Res 61/295).
2. Directive 95/46/EC, 1995 O.J. (L 281) 31 and the EU General Data Protection Regulation.
3. *Ahuriri-Driscoll A.,* Enacting Kaitiakitanga: Challenges and Complexities in the Governance, 2014.
4. *Callison C.,* Material Culture in Flux: Law and Policy of Repatriation of Cultural Property, University of British Columbia Law Review, Special Issue, 1995, 165-181.
5. *Campbell D. T.,* Common Fate, Similarity and other Indices of the Status of Aggregates of Persons as Social Entities, Behavioral Science, 1958, <https://doi.org/10.1002%2Fbs.3830030103> [12.11.2025].
6. *Coll T., Taylor J. (eds.),* Indigenous Data Sovereignty: Toward an Agenda, 2016.
7. Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), *Feasibility Study*, 17/12/2020, <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> [12.11.2025].
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, 5/12/2024, <https://rm.coe.int/1680afae3c> [12.11.2025].

9. Council of Europe, Overview of the Council of Europe Activities in the Field of Artificial Intelligence, <https://rm.coe.int/brochure-artificial-intelligence-en-march-2023-print/1680aab8e6> [12.11.2025].
10. Co-designing Māori Data Governance, (Stats NZ) Data.gov.nz, Fata toolkit, <https://data.govt.nz/toolkit/data-governance/maori/> [12.11.2025].
11. *Dixon P., Milanes V., et al.* The Twin Transition from a Global Perspective: Framing the Debate. Presentation of Preliminary Research regarding the Twin Transition - Summary Report from a Series of Global Roundtables. OECD Ministerial Meeting, Gran Canaria Span. World Privacy Forum and ADC tor los Derechos Civiles. 13/12/2022, <https://www.worldprivacyforum.org/wp-content/uploads/2022/12/Twin_Transition_Report1_WPF_ADC_13December2022_fs.pdf> [12.11.2025].
12. *Erueti A.,* the UN Declaration on the Rights on Indigenous Peoples: A New Interpretive Approach, Oxford University Press, 2022.
13. *Gonzalez C. G.,* Environmental Justice, Human Rights and the Global South, 13 Santa Clara Journal of International Law 151, 2015.
14. *Helfer L. R., Austin G. W.,* Human Rights and Intellectual Property: Mapping the Global Interface, Cambridge University Press, 2011, rev. 2017.
15. *Karjala D. S.,* Robert Kirkwood Paterson, Looking beyond Intellectual Property in Resolving Protection of Intangible Cultural Heritage of Indigenous Peoples, Cardozo Journal of International and Comparative Law, Vol. 11, 2003, 633.
16. *Kukutai T., Campbell-Kamariera K., Mead A., Mikaere K., Moses C., Whitehead J., Cormack D.,* Māori Data Governance Model Te Kāhui Raraunga, <https://tengira.waikato.ac.nz/__data/assets/pdf_file/0008/973763/Maori_Data_Governance_Model.pdf> [12.11.2025].
17. Maori Sovereignty Network, Te Mana Raraunga, Māori Data Audit Tool, <https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/59152b7db8a79bdb0e64424a/1494559615337/Māori+Data+Audit+Tool.pdf> [12.11.2025].
18. Māori Data Sovereignty Network, Te Mana Raraunga, the <https://www.temanararaunga.maori.nz> [12.11.2025].
19. *Mercredi O.,* Aboriginal Languages Celebrated, Saskatchewan Indian, Vol. 22, no. 4, 1993, 8.
20. Model Development Lifecycle (MDL) Item 22, 13, <https://www.msd.govt.nz/documents/about-msd-and-our-work/work-programmes/initiatives/phrae/mdl-governance-guide-for-effective-operational-algorithm-decision-making.pdf> [12.11.2025].
21. *Ouden D. A. E., O'Brien J. M.,* Recognition, Sovereignty Struggles, and Indigenous Rights in the United States: A Sourcebook, University of North Carolina Press, 2013.

22. *Phillips J.,* Australia's Heritage Protection Act: An Alternative to Copyright in the Struggle to Protect Communal Interests in Authored Works of Folklore, Pacific Rim and Policy Journal, Vol. 18 no. 3, 2009, 547-573.
23. Presentation of Jong-Sung Hwang, President, National Information Society Agency on Korea's Digital Bill of Rights and Evolution of Digital Inclusion and Presentation by Tahu Kukutai, Māori Data Governance Model, Data for Self Determination, at OECD event: Presentation of Charter on the Values and Principles for a Digital Shared Prosperity Society: Digital Bill of Rights, The Government of the Republic of Korea, 2023.
24. Remarks of Terina Fa'agau Devin Kamealoha Forrest, Presentation for Privacy tutorial hosted by World Privacy Forum and WACV Conference: AI Governance and data protection: Problem solving for Computer Vision and more, WACV conference, Hawaii, 8/01/2024.
25. *Skogstad L.,* Whose Artificial Intelligence? Design Assembly, <https://designassembly.org.nz/2023/05/08/whose-artificial-intelligence-reflecting-on-the-intersection-of-ai-and-te-ao-maori/> [12.11.2025].
26. The Government of New Zealand, Te Ao Māori Framework, Te Anga Ao Māori, <https://www.hqsc.govt.nz/assets/Misc/Te_Ao_Maori_Framework_FINAL.pdf> [12.11.2025].
27. The Government of New Zealand, Te Ao Māori Framework Implementation Guide, <https://www.hqsc.govt.nz/assets/Misc/Implementation_guide_Te_Ao_Maori_Framework_FINAL.pdf> [12.11.2025].
28. The First Nations Principles of OCAP, First Nations Information Governance Centre, <https://fnigc.ca/ocap-training/> [12.11.2025].
29. *Tsosie,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019)
30. U.S. Indigenous Data Sovereignty Network, <https://usindigenousdatanetwork.org/resources/> [12.11.2025].
31. Visit to Costa Rica – Report of the Special Rapporteur on the rights of indigenous peoples, A/HRC/51/28/ Add.1, United Nations. Human Right Council Fifty-first session, 12 Sept - 7 October 2022, <https://www.ohchr.org/en/documents/country-reports/ahrc5128add1-visit-costa-rica-report-special-rapporteur-rights-indigenous> [12.11.2025].
32. *Walter M., Kukutai T.,* Indigenous Data Sovereignty and Policy, Routledge: London, 2020.

Giuseppe D'Acquisto*

Ludovica De Benedetti**

A Framework for Privacy-Enhancing Technologies Implementations in Trustworthy Data Sharing***

1. The Concept of Data Sharing

Data represent essential assets for organizations, enabling them to pursue their specific objectives and to generate direct value. For instance, data may be collected and analyzed to improve customer experiences, optimize business operations, or foster innovation in the organization's interest.

However, the value of data frequently extends beyond the organizations that originally collect and use them. When combined with other sources, data can generate new insights, support the development of novel products and services, and stimulate both social and economic growth. In this way, additional value can be extracted from the same dataset, beyond its initial purpose.[1]

Based on this observation, many organizations have promoted the concept of "data sharing" which can take the form of internal data governance strategies within a single company or legally defined frameworks at the national or international level.[2] According to the OECD, data sharing "refers to the act of providing data access for use by others, subject to applicable technical, financial, legal, or organisational use requirements"[3]. "It includes the re-use of data based on commercial and non-commercial conditional data-sharing agreements, as well as open data."[4]

* Garante per la Protezione dei Dati Personali Italian Data Protection Authority.

** Institute of International Legal Studies (ISGI), Consiglio Nazionale delle Ricerche (CNR) - Italy.

*** The paper is the text of a keynote speech presented within the framework of the 75th meeting of the International Working Group on Data Protection in Technology, held in Tbilisi and hosted by the Personal Data Protection Service.

[1] According to the Organization for Economic Cooperation and Development (OECD), data access and sharing can help generate social and economic benefits worth between 0.1% and 1.5% of gross domestic product (GDP) in the case of public-sector data, and between 1% and 2.5% of GDP when also including private-sector data (https://www.oecd.org/digital/data-governance/). The EU Commission forecasts that the value of the data economy in the EU27 area is expected to reach €829 billion by 2025, up from €301 billion in 2018 with a compound annual growth rate (CAGR) of more than 14% <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en> [01.06.2024].

[2] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, 2019 <https://doi.org/10.1787/276aaca8-en> [15.09.2025].

[3] *OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463, 2021* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463> [15.09.2025].

[4] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, 2019 <https://doi.org/10.1787/276aaca8-en> [15.09.2025].

By gathering more extensive and diverse datasets, organizations can drive innovation and growth also in a broader, societal interest. For example, when healthcare providers share data with researchers, it can improve the accuracy of diagnoses and lead to more effective treatments. In the same way, when public authorities share data, it can facilitate better coordination and response to crises such as pandemics or natural disasters. As a further example, data sharing can enable businesses gain new insights and develop new products and services for the public benefit, which they would not have been able to create otherwise. This can enhance competitiveness and foster job creation. Therefore, data sharing has the potential to enhance decision-making processes, improve outcomes, and ultimately benefit society as a whole.

At the same time, data sharing may entail risks and adverse effects for persons impacted by the use of data. Beyond individual harms such as privacy violations, one of the most pressing concerns is *group discrimination*[5]. This occurs when shared datasets are used in ways that create new forms of discrimination or reinforce or exacerbate biases against particular social groups, whether defined by ethnicity, gender, age, socio-economic status, or other characteristics. Even when data are anonymized, patterns and correlations can lead to the identification of groups that are then subject to differential treatment. For example, algorithmic decision-making based on shared datasets may disadvantage certain communities in access to credit, healthcare, or employment opportunities[6]. This can occur due to data contamination resulting from historically skewed datasets or subjective class labeling introduced by data miners. Additionally, there may be collection bias resulting from systematic under- or over-representation of particular groups, potentially resulting in discriminatory or unequal treatment[7].

In fact, the risks arising from data sharing are not limited to intentional misuse but can also arise from seemingly neutral practices, such as data model design or training dataset selection. Therefore, addressing the risk of different types of potential discrimination requires proactive safeguards, including bias audits, equity assessments, and inclusive governance structures.

At the same time, data sharing often involves the processing of personal data, which means information that relates to an identified or identifiable individual. The practice of data sharing itself does not automatically entail data protection issues, but by the mere fact that the sharing involves a processing of personal data, strict adherence to data protection principles is indispensable. Respecting these principles safeguards the trust between data producers and users—a precondition for

[5] *Favaretto M., De Clercq E. & Elger B.S.,* Big Data and discrimination: perils, promises and solutions. A systematic review, J Big Data 2019, 6-12 <https://doi.org/10.1186/s40537-019-0177-4> [01.09.2025].

[6] *d'Alessandro B., O'Neil C., La Gatta T.,* Conscientious Classification: a Data Scientist's Guide to Discrimination-Aware Classification, Big Data, 2017, 5(2), 120–34. *Schermer BW.*, The Limits of Privacy in Automated Profiling and Data Mining, Comput Law Secur Rev. 2011, 27(1), 45–52. *Kroll JA., Huey J., Barocas S., Felten EW., Reidenberg JR., Robinson DG., Yu HL*., Accountable algorithms, Univ Pa Law Rev. 2017, 165(3), 633–705.

[7] *Brayne S.,* Big Data surveillance: the case of policing, Am Sociol Rev. 2017, 82(5), 977–1008. *Barocas S., Selbst AD.,* Big Data's disparate impact. California Law Rev. 2016, 104(3), 671–732.

generating significant economic value. Moreover, when processing personal data "for the public benefit," it is crucial to ensure that such processing remains proportionate to the underlying public interest objective.

By upholding data protection principles, organizations not only mitigate the risks of data misuse, but create a conducive environment for innovative collaborations and value generation.

In fact, appropriate data handling is crucial for unlocking the full value of data, since it can establish a sense of trust with the public, which is a prerequisite for the public acceptance of data sharing activities. Individuals that are involved in data sharing activities want to have the reasonable expectation that their data will be utilized for ethical and legitimate purposes.

An important strategy in this regard is the "by-design" approach[8] which requires embedding data protection and ethical considerations into the design of data systems from the outset. By adopting this approach, organizations can strengthen their data governance practices, build trust with data subjects, and enable more responsible and effective data sharing.

Following this approach, a set of technical and organizational arrangements, collectively known as Privacy-Enhancing Technologies (or PETs), are available at various levels of maturity.[9] These technologies aim at reducing privacy risks when sharing data, including sensitive or confidential information, thereby supporting responsible innovation.

This article will examine the legal instruments that foster data sharing, the risks associated with such practices, and the safeguards provided by data protection laws. Particular attention will be devoted to Privacy-Enhancing Technologies as both legal and technical instruments for trustworthy data sharing, along with a series of recommendations for those engaging in these activities.

2. Legal Instruments Promoting Data Sharing

There is a growing worldwide interest among legislators in regulating data sharing, reflected in a significant number of legislative and policy initiatives at both national and supranational levels. This trend stems from the recognition that data are key enablers of innovation, economic competitiveness, and public welfare, but that their sharing raises important legal, ethical, and social challenges. Already back in 2019 the OECD had identified over 200 government-led initiatives in more than 30 countries aimed at promoting data sharing. Most of these initiatives (almost 65%) focus on the sharing of data held by the public sector, but a significant share (around 15%) has the

[8] Art. 25, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR).

[9] The United Nations guide on Privacy-Enhancing Technologies for official statistics. United nations Big Data 2023 <https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf> [25.09.2025].

goal of facilitating data sharing within the private sector. Notably, nearly half of these initiatives involved the sharing of personal data, thereby triggering complex issues of compliance with data protection and privacy frameworks[10].

In the following, we present some examples of recent initiatives that aim at governing the collection, processing, and transfer of (national) data-sets:

- The European Union has recently implemented two legislative initiatives, the European Data Governance Act[11] and the EU Data Act[12], aimed at promoting data sharing in the public and private sectors. The European Data Governance Act facilitates data sharing by establishing a set of measures that include the creation of data intermediaries and processing environments, as well as new contractual arrangements between the public sector and the re-user. Similarly, the EU Data Act sets up rules for data exchange, removes contractual imbalances, and defines circumstances under which public sector bodies may access and use data held by private companies for general interest purposes.
- The "Data Availability and Transparency Act 2022" (Australia)[13] establishes a data sharing scheme under which Commonwealth bodies are authorised to share their public sector data with accredited users, and accredited users are authorised to collect and use the data, in a controlled way[14].
- The "Data Sharing Governance Framework" (2022, UK) [15] sets out guidelines for data sharing among public sector bodies in the UK, while taking into account technical (compatibility with legacy systems, differing data formats) and organizational barriers to such sharing.
- The "National Strategy to Advance Privacy Preserving Data Sharing and Analytics" (2023, USA) aims at substantially advancing Data Sharing and Analytics among public sector bodies of the US Federal Government[16].

---

[10] *The World Economic Forum*, *Good Data: Sharing Data and Fostering Public Trust and Willingness*, p. 6, 2021 <www.weforum.org/whitepapers/good-data-sharing-data-and-fostering-public-trust-and-willingness/> [10.09.2025] and *Organization for Economic Co-operation and Development, Economic and social benefits of data access and sharing* - in *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Chapter 3, OECD Publishing, 2019 <www.oecd-ilibrary.org//sites/276aaca8-en/1/2/3/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book> [15.09.2025].

[11] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1–44. <https://eur-lex.europa.eu/eli/reg/2022/868/oj> [15.09.2025].

[12] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 22.12.2023, p. 1-71. <https://eur-lex.europa.eu/eli/reg/2023/2854> [15.09.2025].

[13] Australian Data Availability and Transparency Act 2022 <www.datacommissioner.gov.au/law/dat-act> - Legal-Text available at: <www.legislation.gov.au/C2022A00011/latest/text> [01.06.2025].

[14] Sections 8 – 13 of the complementary "Data Availability and Transparency Act 2022" list "circumstances in which (data) sharing is barred".

[15] UK, Data Sharing Governance Framework, 2022 <www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework> [01.06.2025].

[16] Table 1 on Page 15 of this National Strategy lists technologies suitable for Privacy Preserving Data Sharing and Analytics.

- In contrast, China has recently adopted a series of measures focusing on the regulation of cross-border data flows. These include the Measures for the Standard Contract for the Outbound Transfer of Personal Information (effective 1 June 2023)[17], the Regulations on Facilitating and Regulating Cross-Border Data Transfers (effective 22 March 2024)[18], and the Network Data Security Management Regulation (Network Data Regulation) (effective 1 January 2025)[19]. Together, these instruments reflect a restrictive and sovereignty-centered approach, seeking to assert state control over data while providing a legal structure for outbound data transfers.
- Saudi Arabia's Data Sharing Policy (سياسة مشاركة البيانات)[20] approved in 2024, issued by the Saudi Data and AI Authority (SDAIA), sets a comprehensive framework for secure and responsible data sharing. It establishes clear rules for government data exchange through the Government Service Bus and the Data Marketplace, introduces strict authorization and classification requirements, and defines safeguards for legality, security, transparency, and ethical use. The policy also sets binding timeframes for processing requests, mandates record-keeping and compliance with the Personal Data Protection Law, and empowers SDAIA to oversee implementation and enforcement.

Taken together, these initiatives illustrate both commonalities and divergences in global approaches to data sharing. While the EU and Australia focus on fostering trust and creating regulated mechanisms for re-use of data, the UK emphasizes governance and flexibility, the U.S. highlights technological solutions for privacy-preserving sharing, China adopts a sovereignty-based model prioritizing state oversight, and Saudi Arabia stresses a rule-based, principle-driven system centred on security, ethical use, and intergovernmental coordination through SDAIA. Despite these differences, the common denominator is the recognition that data sharing must

[17] China, Measures for the Standard Contract for the Outbound Transfer of Personal Information, Cyberspace Administration of China, Decree No. 13 (effective 1 June 2023). Text available at the following link: <https://appinchina.co/government-documents/measures-for-the-standard-contract-for-outbound-transfer-of-personal-information/?utm_source=chatgpt.com> [20.09.2025].

[18] China, Provisions on Facilitating and Regulating Cross-Border Data Flow (effective 22 March 2024). Text and commentary available at: <www.chinalawupdate.cn/2024/04/articles/data-privacy/china-issues-regulations-on-facilitating-and-regulating-cross-border-data-flow/?utm_source=chatgpt.com> and <www.loc.gov/item/global-legal-monitor/2024-05-13/china-new-rules-on-cross-border-data-transfers-released/?utm_source=chatgpt.com> [20.09.2025].

[19] Regulation on Network Data Security Management (effective 1 January 2025), State Council Decree No. 790. Text available at the following link: <https://appinchina.co/government-documents/regulation-on-network-data-security-management/?utm_source=chatgpt.com> [20.09.2025]; official translation in English <https://english.www.gov.cn/policies/latestreleases/202409/30/content_WS66fab6c8c6d0868f4e8eb720.html?utm_source=chatgpt.com> [20.09.2025].

[20] SDAIA, Data Sharing Policy, 2024 <https://sdaia.gov.sa/en/SDAIA/about/Documents/DataSharingPolicyEN.pdf> [22.09.2025].

be actively governed, not only to unlock its potential for innovation and growth but also to address risks to privacy, fairness, and national security.

Nevertheless, the lack of harmonised approaches across countries—especially concerning personal and confidential data—continues to limit cross-border access and interoperability. This gap persists despite international calls, such as the OECD Recommendation on Enhanced Access and More Effective Use of Public Sector Information (2008)[21], the OECD Cancún Declaration on the Digital Economy (2016)[22], and the G20 Digital Economy Ministerial Declaration (2024)[23], all of which emphasise the importance of developing international arrangements and interoperable privacy frameworks to facilitate secure and trusted data flows across jurisdictions.

3. The Legal Architecture of Data Sharing

Data sharing is not an unregulated option within the framework of personal data processing. On the contrary, it is embedded in a dense web of international and regional legal norms that require any data-sharing practice to be respectful of fundamental data protection principles and of the rights of individuals. These obligations can be derived from several international instruments, most notably the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, revised 2013), and more generally, the right to privacy as enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention on Human Rights (ECHR).

At the global level, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (first adopted in 1980 and revised in 2013) remain one of the earliest and most influential attempts to provide a coherent framework for cross-border data flows. These Guidelines establish foundational principles such as purpose specification, data minimization, and accountability, and continue to inform both national legislation and international negotiations[24].

Similarly, within the United Nations framework, the right to privacy under Article 17 of the International Covenant on Civil and Political Rights (ICCPR) has been increasingly interpreted as extending to digital environments, thereby placing limits on the ways personal data may be shared or transferred across jurisdictions[25]. The UN General Assembly has also adopted multiple resolutions recognizing the importance

[21] *OECD, Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, OECD, Paris, 2008* <https://legalinstruments.oecd.org/public/doc/122/122.en.pdf> [22.09.2025].
[22] *OECD, Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration), OECD, Paris, 2016* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0426> [22.09.2025].
[23] G20 Digital Economy Ministerial Conference, 2024 <https://www.g20.utoronto.ca/2024/240913-digital-ministerial-declaration.html> [15.09.2025].
[24] *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013 Revision. OECD, Explanatory memoranda of the OECD Privacy Guidelines, 2022, PP 11-12.*
[25] International Covenant on Civil and Political Rights (Adopted by General Assembly resolution 2200 (XXI) of 16 December 1966) (ICCPR), Art. 17: Right to privacy.

of protecting privacy in the context of digital communications and cross-border surveillance, which indirectly shape global debates on data governance[26].

At the regional level, Europe has been at the forefront of regulatory developments. The Council of Europe's Convention 108 (1981 revised in 2018) is the only binding international treaty on data protection and explicitly covers transborder data flows while requiring Parties to ensure adequate protection standards in case of cross-border transfers[27]. Within the European Union, the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) provides a comprehensive framework for data processing and sets strict conditions for international data transfers. Beyond Europe, other regional organizations have also advanced regulatory frameworks.[28]

These tools demonstrate that data sharing is no longer regulated exclusively at the national level, but is increasingly embedded in a complex network of international, regional, and plurilateral frameworks. This normative architecture not only shapes national legislation but also provides the baseline principles (lawfulness, fairness, accountability, security, and proportionality) that States must take into account when designing their own policies.

These international standards include a series of requirements for data controllers. First, they are required to establish consistent and robust data governance frameworks to ensure that personal data is managed in a responsible and ethical manner.[29] Such frameworks should be accompanied by comprehensive risk assessments aimed at identifying potential risks associated with data sharing. These include privacy and data protection impact assessments (PIAs/DPIAs), which help to evaluate the potential privacy risks and identify appropriate mitigation measures[30].

Data controllers are also required to adopt clear policies and procedures for data retention and disposal, ensuring that personal data is not kept longer than necessary and is securely disposed once it is no longer needed. To guarantee accountability, they should conduct regular audits and reviews of the data-sharing process to verify compliance with applicable legal and regulatory requirements.

Another crucial element is transparency towards individuals, which involves notifying data subjects when their personal data is being shared and providing them

[26] UN General Assembly Resolutions on the right to privacy in the digital age, e.g., A/RES/68/167 (2013).
[27] Council of Europe, Convention 108, 1981; modernized as Convention 108+, 2018, Arts. 5–7.
[28] The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014) sets out obligations for member states on data sharing and data transfers, while in the Asia-Pacific region, the APEC Cross-Border Privacy Rules (CBPR) system establishes a voluntary, enforceable mechanism for facilitating trusted data flows among participating economies. At the bilateral and plurilateral level, several trade agreements—such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the USMCA (United States–Mexico–Canada Agreement)—include provisions on cross-border data flows, which indirectly regulate data sharing by prohibiting unjustified restrictions while requiring safeguards for personal information.
[29] Convention 108+ (Art. 10) explicitly requires controllers to adopt appropriate safeguards, while the GDPR (Art. 24) imposes the principle of accountability, obliging controllers to demonstrate compliance.
[30] Both Convention 108 (Art. 10(3)) and the GDPR (Art. 35) mandate the use of Data Protection Impact Assessments (DPIAs) where processing is likely to result in high risks to individuals' rights and freedoms. The OECD Guidelines similarly emphasise risk-based approaches to personal data flows.

with information about their rights, including the right to access and correct their data. At the same time, the accuracy and quality of data must be improved through mechanisms such as data validation or, where appropriate, age verification.

In addition, controllers must carry out necessity and proportionality tests to minimize the volume of personal data transferred to other organizations, thereby reducing the risk of breaches and privacy violations. They must also establish procedures for preventing and responding to data breaches or other security incidents, while implementing mitigation measures to protect affected individuals.

Equally important is the adoption of multilateral data sharing agreements that clearly define the purpose, scope, and terms of sharing, including limitations on the use of shared data, confidentiality obligations, and prohibitions against unauthorized re-identification. These agreements should be supported by training programs, fostering awareness of the risks associated with data sharing promoting knowledge and skills necessary to manage them effectively.

Finally, controllers are expected to implement data portability mechanisms that empower data subjects to receive their personal data in a structured, commonly used, and machine-readable format, or to transmit those data directly to another controller.

4. Data Protection Risks in Data Sharing

The potential value of collaboration must always be carefully assessed based on its implications for privacy, data security, and the control of sensitive corporate data. There are several risks associated with the concept of data sharing that must be addressed to ensure the protection of personal data, not only to protect the rights of individuals but also to ensure the trust necessary for sustainable collaboration between organizations[31].

One of the foremost challenges lies in the lack of awareness from data subjects and the public regarding the fact that the data is processed, its purpose, the legal basis, the business model (which use-cases are envisaged for the 'data space'/'data sharing', including the societal impact in terms of fostering economic inclusion and mutualization[32]).

This lack of awareness, mostly generated by transparency issues, runs counter to the principle of fairness and lawfulness at the international and regional levels[33] both of which require that data subjects be clearly informed of processing activities that concern them. The OECD Guidelines on the Protection of Privacy and Transborder

[31] *OECD,* Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019 <https://doi.org/10.1787/276aaca8-en> [20.09.2025].

[32] See for instance *Assessment of current and future impact of Big Data on Financial Services*, 2016, available at <https://finance.ec.europa.eu/system/files/2016-12/1606-big-data-on-financial-services_en_0.pdf> [06.09.2025].

[33] Two emblematic examples are Article 5(4)(a) of Convention 108 and, at a regional level, Article 5(1)(a) of the General Data Protection Regulation 2016/679 (GDPR).

Flows of Personal Data also enshrine transparency as fundamental principles for cross-border data flows[34].

A further concern is the lack of fairness in data handling, often resulting from insufficient technological or organizational safeguards. Without adequate mechanisms to make processing understandable and explainable, individuals may be subjected to opaque data practices that prevent them from exercising meaningful control. Closely related is the lack of purpose limitation. In many collaborative data-sharing contexts, the scope of processing is vaguely defined, with activities driven by casual discovery rather than a structured, hypothesis-based or scientific approach. This practice conflicts with the principle of purpose limitation for which data could be processed only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[35].

Even where individuals and organizations explicitly agree to specific terms for data sharing and reuse, including the purposes for which data may legitimately be reused, there remains a significant risk that third parties may intentionally or unintentionally repurpose the data in ways that deviate from the agreed framework. The widely discussed Cambridge Analytica case exemplifies this risk: Facebook users' personal data, initially collected with the understanding that they would be used for academic research, were subsequently exploited for commercially motivated political campaigning. This occurred despite Facebook's explicit prohibition on selling or transferring data to "any ad network, data broker or other advertising or monetization-related service"[36].

The Cambridge Analytica incident is only one among many instances where data have been repurposed in contexts that violate the original terms and conditions. Crucially, such violations are not always the result of malicious intent. Data sharing involves the extraction of data from one context and their transfer into another. As can be understood by also referring to Nissenbaum's theory[37] of privacy as contextual integrity, any change in context makes it difficult to ensure the maintenance of existing rights and obligations. For example, the privacy assumptions and expectations implicit in the initial use of data may no longer apply to subsequent reuse. The risks associated with data reuse depend on the context in which the data was collected and the new context in which it will be used. Therefore, data sharing and its use for additional purposes must be embedded in a robust framework of transparency, accountability, and safeguards.

[34] *OECD,* Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, Part Two: Basic Principles of National Application.
[35] This principle is provided for example in OECD Guidelines, Article 5(4)(a) of Convention 108 and Article 5(1)(b) GDPR.
[36] *Granville K.,* Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, The New York Times, 2018; Isaak J. and Hanna M., User data privacy: Facebook, Cambridge Analytica, and Privacy Protection, Computer, Vol. 51/8, pp. 56-59, 2018.
[37] *Nissenbaum H*., Privacy as Contextual Integrity, Washington Law Review, Vol. June, 2004.

The risks also extend to the duplication and dissemination of data beyond lawful or legitimate purposes, which can undermine the principles of both storage limitation and purpose limitation. Furthermore, inefficient or unnecessary use of data often occurs. This phenomenon, which can be described as "data waste," not only leads to inefficient resource allocation but also violates the principle of data minimization[38] and is closely linked to increased data security risks.

Security is, in fact, another critical concern. Large-scale data sharing often involves the transmission of data across multiple networks and systems, each managed by different organizations with different policies. This increases the likelihood of security incidents and data breaches, potentially compromising confidentiality, integrity, and availability[39]. In addition, unlawful access or disclosure becomes a heightened risk as data are exchanged across multiple organizations and systems and in these cases, the difficulty of establishing consistent governance frameworks across jurisdictions or sectors can further compromise the lawfulness of processing.[40]

A reduction in data quality is equally problematic, as it can lead to incorrect decisions and discriminatory outcomes. The heterogeneity of data sources, if not properly addressed, can result in inconsistencies and errors, thereby violating the principle of data accuracy.[41] This inaccuracy may also affect fairness, particularly when automated decision-making is involved, potentially amplifying bias and discrimination.

The principle of accountability, which requires proactive behavior and the demonstration of concrete measures to ensure the protection of personal data, also becomes more complex to implement in data-sharing contexts. When multiple organizations are involved in complex processing operations, it is often unclear how responsibilities are divided between data controllers and processors[42]. This uncertainty complicates the enforcement of regulations and weakens the effectiveness of regulatory frameworks for accountability.[43]

Ultimately, all data protection principles are implicated in data sharing. The only sustainable, legally and workable concept of data sharing is the one where these principles are preserved. If correctly implemented in a substantial, genuine and not purely formal way, data protection principles are not obstacles but rather enablers of responsible sharing. The principle of necessity and proportionality offers the legal base to reconcile innovation and fundamental rights. It requires a balancing of the effectiveness of the data sharing to pursue the stated objective, on the one hand, with the interference with privacy and data protection, on the other hand.[44]

---

[38] Convention 108, Art. 5(4)(c) and GDPR, Art. 5(1)(c).

[39] *OECD*, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019.

[40] Convention 108+, Art. 5(4)(a); GDPR, Art. 5(1)(a).

[41] Article 5(4)(d) Convention 108; Article 5(1)(d) GDPR.

[42] *European Data Protection Board (EDPB),* Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.0, 7 July 2021.

[43] Convention 108+, Art. 10; GDPR, Arts. 24–28.

[44] This principle is explicit in European Convention on Human Rights, Rome, 4.XI.1950, Article 8(2) (ECHR) and in ICCPR Article 17, and further operationalized in EU law through the GDPR's provisions.

The assessment of concrete risk-mitigation measures, such as the adoption of Privacy-Enhancing Technologies, strict purpose limitation, or robust contractual frameworks, is part of this balancing test. By ensuring compliance with international and regional data protection standards, data sharing can support innovation while also building the trust and legal certainty necessary for collaboration, value creation, and societal benefit. In this sense, data protection legislation acts not as an obstacle, but as a facilitator of data sharing, offering a principled and legally predictable framework to reconcile technological progress with the fundamental rights of individuals.

5. Privacy-Enhancing Technologies as Legal and Technical Instruments for Trustworthy Data Sharing

A consolidated set of technologies called Privacy-Enhancing Technologies (or PETs) have the potential to fundamentally redefine the dynamics of data-sharing by eliminating – or greatly reducing – the risks historically associated with collaboration and data sharing in many practical use cases. Most PETs are mature enough to enable the exploration of previously inaccessible opportunities[45].

Traditional models of collaboration typically rely on merging local datasets into a single dataset that is then made accessible to all participants. Today, however, technological advances enable a shift beyond this rather simplistic conception of data sharing. Modern approaches make it possible to carry out computations and other logical operations at the core of data processing while minimizing the amount of personal data that must actually be shared. At the same time, they allow for the protection of the data used in these computations against undesired inferences that could be drawn from their results. In this respect, privacy-enhancing technologies (PETs) can play a dual role, safeguarding both input privacy and output privacy.

For input privacy, a range of PETs are available, including private set intersection[46], homomorphic encryption[47], secure multiparty computation[48] and zero

[45] For an overview of the new emerging PETs see *OECD, Emerging privacy-enhancing technologies: Current regulatory and policy approaches, OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, 2023* <https://doi.org/10.1787/bf121be4-en> [01.10.2025] and *Asrow K., Samonas S.,* Privacy Enhancing Technologies: Categories, Use Cases and Considerations, Federal Reserve Bank of San Francisco, CA, 2021.

[46] Private Set Intersection (PSI) is a secure multiparty computation cryptographic technique that allows two parties holding sets to compare encrypted versions of these sets to compute the intersection. In this process, neither party reveals anything to the other except for the elements in the intersection.

[47] Homomorphic Encryption (HE): enables computations to be performed directly on encrypted data, producing an encrypted result that can be decrypted later, without ever exposing the underlying raw data.

[48] Secure Multiparty Computation (SMPC) allows multiple parties to jointly compute a function over their inputs while keeping those inputs private from one another.

knowledge proofs[49]. Instead, the output privacy problem can be tackled with two additional PETs: randomization[50] and generalization[51].

PETs that provide input privacy can significantly reduce the number of parties with access to personal information. Input privacy means that the party carrying out logical or numerical operations on personal data cannot access the personal data in clear, access intermediate values or statistical results during processing (unless the value has been specifically selected for sharing); or derive inputs by using techniques such as side-channel attacks that use observable changes during processing (e.g. query timings or power usage) to obtain the input.

Input privacy techniques normally involve the initial transformation of data and computations through encryption mechanisms. For example, when using Secure multiparty computation (SMPC), data are typically split into multiple components or shares, which are then combined to perform computations[52].

One example of input privacy can be found in the reconciliation of trade data across international borders. Using secure multiparty computation techniques such as private set intersection, a country's import data can be compared with the corresponding export data of its trading partner. In this way, both sides can identify consistencies or discrepancies without ever disclosing transaction-level trade information. This enables the exchange of meaningful, coherent insights while preserving the confidentiality of sensitive data. Input privacy techniques such as secure-multiparty computation can be used as an advanced form of pseudonymisation when the inputs are personal data[53].

Other input privacy techniques may involve the creation of trusted execution environments where computations are performed in secure hardware partitions with limited risks for altering the relevant processing operations.

Conversely, output privacy techniques normally adding noise or grouping data into categories can safeguard personal data by preventing individual identification. It is worth noticing that by carefully engineering the level of noise or the amplitude of intervals, data accuracy in the targeted output can often be preserved while making re-identification efforts unreasonable, as per the identifiability criterion outlined, for example, in Recital 26 of the GDPR[54]. In legal terms, these output privacy techniques might be regarded as anonymization techniques.

---

[49] Zero-Knowledge Proofs (ZKPs) is a protocol in which allow one party to prove to another that a statement is true (e.g., that they meet a condition) without revealing any additional information beyond the validity of the statement itself.

[50] Randomization introduces carefully calibrated statistical "noise" into query results so that individual records cannot be singled out, while still allowing useful aggregate analysis.

[51] Data generalization is the process of compressing or summarizing detailed data into higher-level, abstract forms by reducing the complexity of data attributes.

[52] A very interesting application of Secure multiparty computation is the JOCONDE (Joint On-demand COmputation with No Data Exchange) initiative launched in April 2024 by Eurostat to foster the adoption of PETs in the European Statistical System, <https://cros.ec.europa.eu/joconde> [05.09.2025].

[53] *ENISA Data Pseudonymisation:* Advanced Techniques & Use Cases Technical analysis of cybersecurity measures in data protection and privacy - January 2021.

[54] From Recital 26 of the GDPR: "To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time

PETs that provide output privacy reduce the risk that people can obtain or infer personal information from the result of a processing activity. This is regardless of whether the implemented computations or logical operations already provide input privacy. Using a PET that provides output privacy is useful in order to make anonymous statistics publicly available or share the results of an analysis with a large group of recipients.

These types of PETs also help comply with the storage limitation and data minimisation principles[55].

An example of output privacy is a national statistics office adding calibrated noise to census data using differential privacy before publishing, ensuring plausible deniability for individuals while providing meaningful insights. The utilisation of differential privacy as an output privacy technique demonstrates its effectiveness as an approach to anonymisation[56].

Both input and output privacy are critical components of a data sharing framework which protects the personal data which is shared. By engineering input privacy and output privacy techniques, in fact, organizations can implement new types of data processing based on secure or secret computing, creating in this way a unique opportunity to enable and incentivize trustable, legal, and economically beneficial sharing of data, also in the context of international data transfer, in a way that may have been unfeasible otherwise.

Additionally, other PETs exist, not strictly related to input or output privacy, which entail more secure processing and reduce the amount of personal data which is accessed by other parties, thus supporting data protection principles, for example federated learning[57] and the use of synthetic data[58].

6. Recommendations

In the previous sections, the potential and risks associated with data sharing have been highlighted: when two or more organizations engage in collaborative data sharing, they collectively contribute to the formation of a broader and richer data ecosystem with great potential benefits for the community, but also risks to the privacy and rights of individuals and groups. Within such ecosystem, computational methods may reveal new insights and trends about individuals, groups, or society at

required for identification, taking into consideration the available technology at the time of the processing and technological developments".

[55] Information Commissioner's Office, Privacy-enhancing technologies (PETs), June 2023, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf> [05.09.2025].

[56] See Harvard University (n.d.), Differential Privacy, Harvard University Privacy Tools Project, <https://privacytools.seas.harvard.edu/differential-privacy> [02.10.2025].

[57] *Konečnỳ J., McMahan B., Ramage D.* Federated optimization: Distributed optimization beyond the datacentre, arXiv preprint arXiv:1511.03575, 2015.

[58] *El Emam K., Mosquera L., Hoptroff R.,* Practical Synthetic Data Generation: Balancing Privacy and the Broad Availability of Data, O'Reilly Media, 2020.

large. However, traditional approaches, such as bilateral exchange of raw datasets or consolidation into a shared repository accessible to all parties, are inadequate, particularly in contexts characterized by distributed actors and large-scale data flows.[59]

Instead, a multilateral approach, grounded in the systematic adoption of Privacy-Enhancing Technologies (PETs) may be a more future-proof option. By leveraging PETs, stakeholders can build a trusted computational environment that maximizes the benefits of secure and privacy-preserving data exchange while ensuring compliance with established data protection principles.[60]

Building on the organizational obligations imposed on data controllers and the risks inherent in data sharing, as well as the benefits associated with the deployment of Privacy-Enhancing Technologies (PETs), this section turns to the practical implications for governance. Specifically, it outlines recommendations which aim at guiding stakeholders in developing privacy-preserving frameworks for data sharing.

6.1. Recommendations for Controllers

Controllers should begin by carefully assessing the rationale for data sharing, identifying the parties with whom the data will be shared, and ensuring that this has been adequately communicated to the individuals concerned. It is essential that data subjects receive clear, concise, and easily accessible information prior to any processing activity involving the collection or sharing of their personal data[61]. Such information should not be delivered in lengthy terms and conditions but instead be presented in short, straightforward language, with the option to access more detailed explanations. Importantly, individuals must also be provided with a meaningful opportunity to object to such sharing.

Any act of sharing personal data constitutes, by definition, a processing of personal data, and therefore gives rise to legal obligations for the organizations involved. Controllers must adopt a responsible approach to data handling and take all necessary measures to ensure compliance with the applicable data protection laws in every jurisdiction where sharing occurs. This begins with the careful selection of an appropriate legal basis for the data-sharing activity[62].

The deployment of Privacy-Enhancing Technologies (PETs) can play a crucial role in mitigating the risks inherent in data sharing, particularly in relation to high-risk data categories, such as special categories of personal data. Under certain assumptions and jurisdiction-specific conditions, PETs may even enable international data transfers that

[59] *Tene O.and Polonetsky J.,* Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239, 2013.

[60] European Union Agency for Cybersecurity (ENISA), Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, December 2015. European Union Agency for Cybersecurity (ENISA), ENISA's PETs Maturity Assessment Repository, November 2018.

[61] *OECD,* Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013.

[62] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller, WP 217, 9 April 2014.

would otherwise be restricted. Beyond their compliance function, PETs also present business-enabling opportunities, allowing organizations to unlock the benefits of data collaboration while reducing privacy risks[63]. For this reason, their adoption should be approached with care, foresight, and a clear understanding of both their limitations and their potential.

6.2. Recommendations for Lawmakers and Governments

Lawmakers and governments should articulate a comprehensive vision and legal system for data sharing that moves beyond the notion of simple data transfers between organizations, while actively limiting data concentration and excessive centralization[64]. Such a vision must also take into account the broader social and economic implications of data sharing, as well as the potential of Privacy-Enhancing Technologies (PETs) to mitigate emerging risks[65]. Importantly, PETs can also serve as an enabler of competition, by lowering entry barriers and opening digital markets to new actors[66].

Legislative initiatives should therefore aim to establish legal frameworks that explicitly promote the adoption of PETs, encouraging organizations to transition towards more privacy-preserving technologies. At the same time, institutions should invest substantially in research and development to improve the usability, scalability, and efficiency of PETs in real-world applications[67]. Governments can further accelerate adoption by introducing targeted subsidies and incentive schemes that make PET solutions more affordable and accessible[68].

At the strategic level, governmental data policies should prioritize compliance with data protection regulations and support the creation of a robust computing infrastructure with embedded and enforceable safeguards. In this regard, public–private partnerships and the establishment of regulatory sandboxes for collaborative experimentation can play a crucial role in building trust among stakeholders, fostering innovation, and ensuring that high standards of privacy and data protection are maintained[69].

---

[63] *McCarthy N., Fourniol F.,* The Role of Technology in Governance: The Example of Privacy Enhancing Technologies, Data & Policy, 2020.

[64] European Commission, A European Strategy for Data, COM (2020) 66 final, 19 February 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC006> [16.09.2025]

[65] *European Union Agency for Cybersecurity (ENISA),* Readiness Analysis for the Adoption and Evolution of Privacy-Enhancing Technologies (PETs), 2022.

[66] *Organisation for Economic Co-operation and Development (OECD),* Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches, OECD Digital Economy Papers No. 351, 2023.

[67] *OECD, Enhancing Access to and Sharing of Data:* Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2021.

[68] European Commission, Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM (2022) 68 final.

[69] *Truby J. et al.*, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications", European Journal of Risk Regulation, 2021 <www.cambridge.org/core/journals/european-journal-of-risk-

Moreover, there is a growing need for a harmonized international regulatory framework on data sharing. Such a framework would help ensure that the benefits derived from data exchanges are realized globally and that cross-border data flows become simpler and more predictable, while still providing strong and effective safeguards for the rights and freedoms of individuals.

6.3. Recommendations for Technology and Solution Providers

Technology and solution providers should promote transparency by openly sharing information on the functioning of their implemented techniques, enabling individuals to understand how their data are handled[70]. In addition, they should encourage public scrutiny of their algorithms, making their algorithms accessible for review and analysis to build trust and ensure fairness.

Collaboration among players should be promoted to create a computing collaborative/cooperative infrastructure for sharing data with clearly defined rules, where, in particular, data protection rules are prioritized.

Standardized, open solutions should be preferred to proprietary ones, in order to reduce discrepancies among different jurisdictions or areas of the world, and to avoid unfair data processing. In addition, beyond legal obligations, voluntary codes of conduct at the sector level should be broadly adopted to generate trust and to establish industry-wide best practices for data handling, security, and privacy[71].

6.4. Recommendations for the Research Community

Researchers and the academia should provide a broader range of proof of concept use cases for emerging PETs. This can help demonstrate the practical applications and potential benefits in various domains[72].

In addition, more effort should be put on reducing the complexity burden for data controllers entailed by the adoption of PETs, developing guidelines and best practices that make their deployment more manageable[73].

Researchers and the academia should actively engage in critical evaluation and validation of solutions proposed by industry. The aim would be to ensure that industry-

regulation/article/sandboxapproach-to-regulating-highrisk-artificial-intelligenceapplications/C350EADFB379465E7F4A95B973A4977D> [05.09.2025].

[70] *United Nations,* Roadmap for Digital Cooperation*,* 2020, available at: <www.un.org/en/content/digital-cooperation-roadmap> [20.09.2025].

[71] It may also be helpful to adopt guidelines aimed at technical architects and product owners working on projects that involve the sharing or processing of sensitive information, such as those from the *CDEI (n.d.),* PETs Adoption Guide, <https://cdeiuk.github.io/pets-adoption-guide/adoption-guide> [02.10.2025].

[72] *Wang Y. & Kobsa A.,* Privacy-Enhancing Technologies: Classification and Applications, in The Handbook of Privacy and Privacy-Enhancing Technologies, 2018.

[73] *Danezis G. et al.,* Privacy and Data Protection by Design – From Policy to Engineering, Computer Law & Security Review, Vol. 34, Issue 2, 2018.

proposed technologies and approaches meet the required standards of security and privacy[74].

6.5. Recommendations for Data Protection Authorities

Data Protection Authorities should promote the adoption of PETs, creating clear and practical use cases for the implementation of PETs to facilitate their adoption by organizations.

Furthermore, they should advocate for the harmonization of PETs taxonomies and scope to ensure better consistency and understanding of the benefits associated with data sharing and collaboration, and provide guidance and support to encourage privacy-conscious practices[75].

Data Protection Authorities should encourage organizations to align the perceived value of data protection with their actual implementation, and facilitate collaboration and communication between data protection experts and technologists to bridge the existing knowledge gap on PETs[76].

7. Concluding Remarks

Data sharing can create significant economic value for society by enabling innovation, improving decision-making, and promoting collaboration; however, this strategy also entails significant risks and uncertainties, such as unauthorised access, lack of transparency for individuals, inability to exercise data subject rights as the individual may not know who controls their data, purpose creep, which must be addressed through effective governance. In any case, the collection and use of personal data, notably if mandatory, must comply with the well-established principles of necessity and proportionality. In case of processing by private entities, due attention should be paid to all possible risks to fundamental rights and freedoms and interests of the persons concerned, having regard, among others, to non-discrimination, financial and societal exclusion, risks stemming from individuals' or groups' profiling and manipulation risks for both the individual and society as a whole[77].

These risks require the implementation of a variety of measures and approaches, both technical and legal, to evaluate and mitigate privacy risks comprehensively and

[74] *van Blarkom J.J., van Eck B.M.A. & Verhaar P.,* Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents, College bescherming persoonsgegevens, 2003.
[75] *Jurcys P., Corrales Compagnucci M., Fenwick M.,* The Future of International Data Transfers: Managing Legal Risk with a User-Held Data Model, Computer Law & Security Review, Volume 46, September 2022, 105691.
[76] *Gregory Voss W.,* "Cross-Border Data Flows, the GDPR, and Data Governance," Washington International Law Journal, Vol. 29, No. 3, 2020.
[77] *Citron D.K. and Solove D.J.,* Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793, 2022, <https://ssrn.com/abstract=3782222> [18.09.2025].

accurately. If organizations fail to do so, not only they would be in breach of the applicable data protection law and principles, but they would also generate a sense of mistrust in their conduct. The cost of such mistrust might be extremely high and significantly affect the efficiency of society and the economy as a whole, ultimately to the detriment of the essence of data sharing strategies.

Considering the amount of data shared and processed, organizations should be proactive in implementing safeguards for individuals, embracing the "privacy by design" approach since the early stage of deployment of new services. Retrofitting remedies after a wrong design choice, if ever possible, would result not only in direct economic costs, but also in higher indirect costs and further uncertainties that can lead to a loss of acceptance of data sharing strategies by citizens and companies.

All data protection principles may facilitate data sharing scenarios for the public benefit, having a positive impact not only for business but also for society as a whole. These principles need to be implemented in a technology-oriented and effective way, in order to ensure an implementation of the forthcoming laws promoting data sharing both in the public and in the private sectors that complies with the relevant data protection principles and rules. Traditional 'naïve' data sharing approaches, namely unrestricted pooling of datasets accessible and operable by all the contributing organizations, would not enable such compliance. Today a set of well-established PETs have the capacity to fundamentally redefine the way data are shared by reducing or eliminating the risks that have traditionally been associated with collaboration. With these emerging technologies, previously inaccessible opportunities for collaboration can now be explored, while upholding the right to privacy and ensuring data protection at every stage of the data-sharing process.

PETs can be seen as a catalyst for partnership and collaboration, as they address many of the concerns that have hindered data-sharing in the past. Organisations should consider, in the first place, why they are sharing data, who they are sharing it with and whether individuals to whom the data relates have been adequately informed and can effectively exercise their rights; in the second place, by utilizing PETs, organisations can further reinforce the effective implementation of data protection principles using technical instruments capable of minimizing the risks associated with data sharing, thus allowing the creation of mutual trust among the participants in data sharing initiatives. Overall, PETs can play a crucial role in creating a foundation for collaborative decision-making that can benefit society as a whole, and can also be regarded as genuine and effective "partnership enabling technologies"[78].

Their integration within a harmonized and internationally coordinated regulatory framework would ensure that data sharing can deliver its promised economic and social benefits, while safeguarding human rights and trust at the global level.

[78] *The Royal Society,* From privacy to partnership: the role of Privacy Enhancing Technologies in data governance and collaborative analysis, 2023 <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf> [24.09.2025].

Bibliography:

1. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014).
2. *Asrow K. and Samonas S.,* Privacy Enhancing Technologies: Categories, Use Cases and Considerations, Federal Reserve Bank of San Francisco, CA, 2021.
3. Australian Data Availability and Transparency Act 2022.
4. *CDEI (n.d.), PETs Adoption Guide*, <https://cdeiuk.github.io/pets-adoption-guide/adoption-guide> [02.10.2025].
5. China, Measures for the Standard Contract for the Outbound Transfer of Personal Information, Cyberspace Administration of China, Decree No. 13.
6. China, Provisions on Facilitating and Regulating Cross-Border Data Flow (effective 22 March 2024).
7. China Regulation on Network Data Security Management (effective 1 January 2025), State Council Decree No. 790.
8. *Citron D.K., Solove D.J.,* Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793, 2022.
9. Council of Europe, Convention 108 + Convention for the protection of individuals with regard to the processing of personal data, June 2018.
10. Councile of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg, 28.I.1981.
11. *d'Alessandro B., O'Neil C., La Gatta T.,* Conscientious Classification: a Data Scientist's Guide to Discrimination-Aware Classification, Big Data, 2017, 5(2), 120–34.
12. *Danezis G. et al.,* Privacy and Data Protection by Design – From Policy to Engineering, Computer Law & Security Review, Vol. 34, Issue 2, 2018.
13. *El Emam K., Mosquera L., Hoptroff R.,* Practical Synthetic Data Generation: Balancing Privacy and the Broad Availability of Data, O'Reilly Media, 2020.
14. *ENISA,* Readiness Analysis for the Adoption and Evolution of Privacy-Enhancing Technologies (PETs), 2022.
15. ENISA Data Pseudonymisation: Advanced Techniques & Use Cases Technical analysis of cybersecurity measures in data protection and privacy - January 2021.
16. ENISA's PETs Maturity Assessment Repository, November 2018.
17. *ENISA,* Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, December 2015.
18. *European Data Protection Board (EDPB),* Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.0, 7 July 2021.
19. *European Commission*, Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM(2022) 68 final.
20. *European Commission,* A European Strategy for Data, COM(2020) 66 final, 19 February 2020.
21. European Convention on Human Rights, Rome, 4.XI.1950.

22. European Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 22.12.2023, p. 1-71.
23. European Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1–44.
24. European Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
25. *Favaretto M., De Clercq E., Elger B. S.,* Big Data and discrimination: perils, promises and solutions. A systematic review, J Big Data 2019, 6-12.
26. *Financial Services User Group (FSUG),* Assessment of current and future impact of Big Data on Financial Services, 2016.
27. *Granville K.,* Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, the New York Times, 2018.
28. *Gregory Voss W.,* "Cross-Border Data Flows, the GDPR, and Data Governance," Washington International Law Journal, Vol. 29, No. 3, 2020.
29. Harvard University (n.d.), Differential Privacy, Harvard University Privacy Tools Project, <https://privacytools.seas.harvard.edu/differential-privacy> [02.10.2025].
30. International Covenant on Civil and Political Rights (Adopted by General Assembly resolution 2200 (XXI) of 16 December 1966).
31. *Isaak J. and Hanna M.*, User data privacy: Facebook, Cambridge Analytica, and Privacy Protection, Computer, Vol. 51/8, pp. 56-59, 2018.
32. *Jurcys P., Corrales Compagnucci M., Fenwick M.,* the Future of International Data Transfers: Managing Legal Risk with a User-Held Data Model, Computer Law & Security Review, Volume 46, September 2022, 105691.
33. *Konečnỳ J., McMahan B., Ramage D.,* Federated optimization: Distributed optimization beyond the datacentre, 2015.
34. *Kroll J.A., Huey J., Barocas S., Felten EW., Reidenberg JR., Robinson D. G., Yu HL*., Accountable algorithms, Univ Pa Law Rev. 2017, 165(3), 633–705.
35. *McCarthy N., Fourniol F.,* The role of technology in governance: The example of Privacy Enhancing Technologies, Data & Policy, 2020.
36. *OECD*, "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, 2023.
37. *OECD,* Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013 Revision. OECD, Explanatory memoranda of the OECD Privacy Guidelines, 2022, PP 11-12.

38. *OECD*, Recommendation of the Council on, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, OECD/LEGAL/0463, 2021.
39. *OECD,* Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019.
40. *OECD,* Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration), OECD, Paris, 2016
41. *OECD,* Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013.
42. *OECD,* Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, OECD, Paris, 2008.
43. *Nissenbaum H*., Privacy as Contextual Integrity, Washington Law Review, Vol. June, 2004.
44. *Royal Society*, from privacy to partnership: the role of Privacy Enhancing Technologies in data governance and collaborative analysis, 2023.
45. *Schermer B. W.*, The Limits of Privacy in Automated Profiling and Data Mining, Comput Law Secur Rev. 2011, 27(1), 45–52.
46. SDAIA, Data Sharing Policy, 2024
47. *Tene O., Polonetsky J.,* Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239, 2013.
48. *Truby J. et al.*, A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications, European Journal of Risk Regulation, 2021.
49. UK, Data Sharing Governance Framework, 2022.
50. UK Information Commissioner's Office, Privacy-enhancing technologies (PETs), June 2023.
51. UN General Assembly Resolutions on the right to privacy in the digital age, e.g., A/RES/68/167 (2013).
52. United Nations guide on Privacy-Enhancing Technologies for official statistics. United Nations Big Data 2023.
53. *United Nations,* Roadmap for Digital Cooperation, 2020.
54. US National Strategy lists technologies suitable for Privacy Preserving Data Sharing and Analytics.
55. *Van Blarkom J.J., Van Eck B.M.A., Verhaar P.,* Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents, College bescherming persoonsgegevens, 2003.
56. *Wang Y. & Kobsa A.,* Privacy-Enhancing Technologies: Classification and Applications, in the Handbook of Privacy and Privacy-Enhancing Technologies, 2018.
57. *World Economic Forum*, Good Data: Sharing Data and Fostering Public Trust and Willingness, p. 6, 2021.

David Weinkauf*

Working Paper on Large Language Models (LLMs)**

Large language models (LLMs) are extremely large, complex machine learning systems capable of routinely generating highly articulate, plausible-sounding—but not necessarily true—linguistic content in response to queries. This paper provides an in-depth, multifaceted analysis of LLMs to help data protection authorities effectively regulate and respond to the challenges of this new technology. The analysis is undertaken from three perspectives: (1) the technology itself, that is, how LLMs fundamentally work and are developed; (2) the privacy and data protection risks raised by them; and (3) the emerging set of best practices to reduce or eliminate these risks.

***Keywords**: Large language models, artificial intelligence, technical analysis, privacy, data protection, risks, best practices, mitigations.*

1. Introduction

LLMs are mathematical models developed using artificial intelligence (AI) and machine learning (ML) data processing techniques to perform tasks related to natural language. The state of the art has advanced significantly in recent years, with some LLMs demonstrating human- and even expert-level natural language processing capabilities for certain tasks. The observed progress in the field is due mainly to advancements in model architecture and training techniques, combined with exponential increases in model sizes, training data corpora and availability of compute.

Despite their capabilities, LLMs are no technical panacea. Their AI-enabled approach to automating linguistic tasks raises a number of privacy and data protection risks. Some risks stem from design choices in the underlying technology; others from practices relating to the processing of personal information; and still others from

* Ph.D. Conseiller principal en politique technologique. Commissariat à la protection de la vie privée du Canada

** The following is an edited, abridged version of the original working paper authored by the International Working Group on Data Protection in Technology (IWGDPT) or "Berlin Group" published on December 27, 2024, available online at <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-LLMs.pdf?__blob=publicationFile&v=2> [25.11.2025].

inherent limitations in mathematical approaches to machine-based language acquisition and understanding.

The aim of this paper is to provide an in-depth, multifaceted analysis of LLMs from the point of view of privacy and data protection. Just as LLMs are complex technologies that raise various privacy and data protection risks, so any proportionate analysis must view the technology from multiple perspectives. It is not only necessary to analyze LLMs from the point of view of the technology itself, that is, a technical analysis of how LLMs fundamentally work, but equally from the perspectives of the privacy and data protection risks they raise and the emerging set of best practices to reduce or eliminate their risks. Only with an understanding of LLMs from the point of view of these three perspectives—the technology, privacy risks and best practices—can data protection authorities (DPAs) position themselves to effectively regulate and respond to this new situation.

This paper is divided into three sections. In the first section, we provide a technical explanation of LLMs, focusing on the role and functionality of various components at each stage of the LLM development lifecycle. In section 2, we provide an analysis of the various data protection and privacy risks raised by LLMs. Finally, in section 3, we discuss best practices to prevent or mitigate some of the risks of LLMs, framing the discussion in terms of key areas requiring consideration by developers and deployers.

Disclaimer

This paper does not contain legal advice, nor do the views expressed in it necessarily reflect the official policy or position of individual IWGDPT members.

2. What are LLMs?

LLMs are extremely large, complex machine learning systems capable of routinely generating highly articulate, plausible-sounding—but not necessarily true—linguistic content in response to queries on virtually any topic. LLMs consist of hundreds of billions or even trillions of parameters organized across various architectural components. Each component plays a specific role and contributes new functionality to the system. Examples of components include the language vocabulary, word embeddings, context window, multi-head self-attention blocks and feed-forward neural networks.

Collectively, these components form what is known as the “transformer” architecture. Artificial intelligence (AI) models, including LLMs, whose design is based on this architecture are commonly referred to as “transformer” models. For a technical

discussion of the transformer architecture, including a breakdown of the number of parameters, please refer to Appendix A in the original version of this article.[1]

The training lifecycle of LLMs is unlike that of most other machine learning applications. Instead of a single stage of training using one form of machine learning, LLMs typically employ a two-stage training procedure with multiple types of learning. The first stage of training is called "pre-training" while the second is called "fine-tuning/alignment."

In what follows, we will discuss the training procedure of LLMs, providing an analysis of each stage, including a description of the learning method used and functionality contributed by each.

It is important to note that these are not the only stages in the development of LLMs. For example, many LLMs undergo a stage of "red-teaming" before they are deployed, in which a team of security and other subject-matter experts attempt to identify vulnerabilities and opportunities for misuse. However, the stages of the training lifecycle provide an opportunity to discuss many of the unique features of LLMs to better understand their overall functionality.

2.1. Stage 1: Pre-Training

During this initial stage, the goal is to create a general-purpose model with a kind of raw, unrefined ability to continuously predict the next word or sub-word "token" in a sequence of text about a given topic. To do this, the model is trained on extremely large amounts of natural language, typically taken from aggregated sets of scraped websites and/or digitized books.

The pre-training procedure follows a form of "self-supervised" learning. This is similar to supervised learning, except that the labels representing a correct prediction or "ground truth" for the model are taken from the training data itself, rather than relying on external labels added separately to the training data. Because natural language contains its own "correct" next-word predictions, pre-training is able to supervise itself, without the need for additional human-generated labels.

Pre-training consists of a series of steps, applied repeatedly across batches of examples until a preset number of training cycles is reached. In general, the training algorithm:

1. samples a sequence of text from the training data;
2. inputs the sequence (minus the last word) into the model to receive a prediction for the next word;
3. calculates the model prediction error for the sequence by taking the difference between the probability distribution of the prediction and that of the actual last word in the sequence; and

[1] See *IWGDPT*, *Working Paper on Large Language Models (LLMs)*, December 27, 2024, <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-LLMs.pdf?__blob=publicationFile&v=2> [25.11.2025].

4. adjusts the value of each parameter in the model (using backpropagation) to reduce the error going forward.

The term "foundation model" is sometimes used to describe the resulting model after the completion of pre-training.[2] However, this term is somewhat controversial. The authors of the paper that coined the term claim to have chosen it to "capture the unfinished yet important status of these models" given their ability "to serve [] as the common basis from which many task-specific models are built via adaptation."[3] Yet, critics have countered that the term is self-serving and misrepresents the nature of the relationship these models have to human language and understanding. One AI researcher in particular stated the following: "These models are really castles in the air. They have no foundation whatsoever."[4]

A more practical and plain-language description can be found outside of academic research. In the words of one AI practitioner, the result of pre-training is a model that "babbles Internet" in the form of a "document completer."[5]

2.2. Stage 2: Fine-Tuning/Alignment

After creating a general-purpose "foundation" model, the next stage in the training procedure of LLMs is to refine the behavior of the model to better "align" its responses with human preferences and values. The desired behavior can be distilled into a set of three criteria, commonly referred to as the three H's: LLMs should act in a manner that is "helpful, honest and harmless."[6]

This is a challenging task. After pre-training, the model is optimized only to continue predicting next words in a sequence. This is a related, but ultimately distinct, task from following user instructions, avoiding falsehoods or refraining from toxic or harmful content. For example, when given a prompt in the form of a user instruction, OpenAI's third-generation generative pre-trained transformer or "GPT-3" simply continues to list examples of similar prompts, whereas the same model but fine-tuned to act as an "InstructGPT" (the precursor to OpenAI's popular "ChatGPT") provides a helpful response. See Table 1 for details.

---

[2] See *Bommasani R., Hudson D., Adeli E. et al.*, On the Opportunities and Risks of Foundation Models, August 2021, <https://doi.org/10.48550/arXiv.2108.07258> [25.11.2025].

[3] Ibid., p. 3 (n. 2) and p. 7.

[4] Quote from *Malik J.* in: *Knight W.*, A Stanford Proposal Over AI's 'Foundations' Ignites Debate, *Wired*, September 2021, <https://www.wired.com/story/stanford-proposal-ai-foundations-ignites-debate/> [25.11.2025]. A video of Malik's remarks is available at <https://www.reddit.com/r/MachineLearning/comments/pd4jle/d_jitendra_maliks_take_on_foundation_models_at/> [25.11.2025].

[5] See *Karpathy A.*, Let's build GPT: from scratch, in code, spelled out, January 2023, <https://www.youtube.com/watch?v=kCc8FmEb1nY> [25.11.2025], at 1:51:45.

[6] See *Askell A., Bai Y., Chen A. et al.*, A General Language Assistant as a Laboratory for Alignment, 2021, <https://doi.org/10.48550/arXiv.2112.00861> [25.11.2025].

Prompt	**Explain the moon landing to a 6 year old in a few sentences.**
Completion	GPT-3: Explain the theory of gravity to a 6 year old. Explain the theory of relativity to a 6 year old in a few sentences. Explain the big bang theory to a 6 year old. Explain evolution to a 6 year old.
	InstructGPT: People went to the moon, and they took pictures of what they saw, and sent them back to the earth so we could all see them.

Table 1: Example of different responses between GPT-3 and InstructGPT for the same prompt. From OpenAI, Aligning language models to follow instructions, <https://openai.com/research/instruction-following> [25.11.2025].

In general, the training procedure of fine-tuning is divided into two (sub)stages. The first follows a form of "supervised" learning, while the second follows a form of "reinforcement" learning.

2.2.1. Supervised Learning

This stage is similar to pre-training, except that the set of examples on which the model is trained are explicitly selected and curated by the developers to demonstrate the type of prompts the LLM is expected to receive and the type of responses it should provide. This is why the training is deemed to be "supervised." The training data contains full examples of task-specific interactions with the LLM, including both the user prompt and the "correct" LLM response.

The amount of training data used at this stage is typically much smaller—in the range of orders of magnitude less—than the amount used during pre-training. The reason for this is due to both practical and scientific considerations. From a practical perspective, creating tailored supervised training datasets is far more resource intensive and time consuming than downloading collections of scraped websites and/or digitized books for use in self-supervised learning, especially given the amount of online digital content available today. Yet from a machine learning perspective, less but high-quality data is actually "more" at this stage. Studies have shown that supervised fine-tuning is "sample efficient," in the sense that comparably less data is needed to train the LLM to perform well on a specific task, such as follow user instructions in a chat-like manner.[7] Thus, using the pre-trained model as a basis,

[7] See *Khandelwal U., Clark K., Jurafsky D. et al.*, Sample Efficient Text-Summarization Using a Single Pre-Trained Transformer, 2019, <https://doi.org/10.48550/arXiv.1905.08836> [25.11.2025].

supervised learning is able to tweak the parameters of the model to transform its raw, unrefined linguistic abilities into more direct and purposeful behavior. After this stage of training, LLMs respond more "helpfully."

2.2.2. Reinforcement Learning

Yet being able to perform a task directly is not the same as being able to perform it responsibly or ethically. While supervised learning can train LLMs to provide more helpful responses, in general, the modifications do not extend to the values of honesty and harmlessness. To gain better alignment with these other values, LLMs typically undergo a second stage of fine-tuning using a technique known as "reinforcement" learning.

Reinforcement learning is a form of machine learning in which a model is trained by interacting in a dynamic environment with feedback, similar to a process of "trial and error." Unlike supervised or self-supervised learning, the model does not learn by way of repeated exposure to examples of "correct" behavior. Instead of a form of imitation, the key pedagogical concept at work in it is that of "reward and punishment." A model is rewarded for behavior that achieves or takes it closer to the goal of the environment and punished for behavior that does the opposite. By exploring different strategies to achieve the goal and updating its parameters based on the positive or negative feedback it receives, the model develops an optimal "policy" that maximizes the reward associated with the environment. Thus, reinforcement learning is more open-ended and exploratory than other forms of machine learning. This is why it is typically used to train models in strategy-based tasks such as games like Go[8] or StarCraft.[9]

In the case of LLMs, the "game" the model is trained to play is that of responding ethically and appropriately to user prompts. While at first blush this may seem like an analogous task to strategic game play, upon closer inspection it becomes clear that ethical decision-making differs in important respects. These differences pose a number of challenges to the application of reinforcement learning within the context of LLMs.

The main challenge is that, unlike strategic games such as Go or StarCraft, there is no precise definition for what constitutes a "win" in ethics. Ethics differs from strategic game play in that it does not occur under the direction of a predefined goal or outcome such as "achieving a high score" or "defeating an opponent." There is no separate, "higher" end or objective under which its actions are subsumed. Ethical action is done for the sake of itself, simply because it is the right thing to do. As Aristotle

[8] See *Silver D., Huang A., Maddison C. et al.*, Mastering the game of Go with deep neural networks and tree search, *Nature*, Vol. 529, 2016, 484–489, <https://doi.org/10.1038/nature16961> [25.11.2025].

[9] See *Vinyals O., Babuschkin I., Czarnecki W. et al.*, Grandmaster level in StarCraft II using multi-agent reinforcement learning, *Nature*, vol. 575, 2019, 350–354, <https://doi.org/10.1038/s41586-019-1724-z> [25.11.2025].

explains the distinction, "the end of making [e.g., strategic game play] is different from itself, but the end of [ethical] action could not be, since acting well is itself the end."[10]

A consequence of this property is that ethical criteria are inherently ambiguous. They do not admit of the same precision as mathematics or the natural sciences. This is a challenge for reinforcement learning because without a precise or well-defined objective, the training process cannot determine whether some action or strategy employed by the model should be rewarded or punished. Since ethical action is its own end, reinforcement learning cannot simply define an external objective by which to evaluate the responses of LLMs.

A second challenge of reinforcement learning within the context of LLMs has to do with the multiplicity of ethical values. The "game" of ethics the model is trained to play does not consist of one value (or "virtue" in Aristotle's terminology) but a combination of three. To respond ethically and appropriately to user prompts, LLMs must act in accordance with the values of helpfulness, honesty and harmlessness.

This raises an additional challenge in that the meanings of these values overlap and conflict with each other, especially when taken to extremes. Due to their inherent ambiguity, instead of being mutually compatible—or in machine learning parlance, mutually "maximizable"—the values of helpfulness, honesty and harmlessness exhibit an inherent tension or tradeoff, where too much of one results in too little of another. This further complicates the task of defining an ethical objective by which to train LLMs using reinforcement learning. In addition to the challenge of programmatically defining ethical values, the "game" of LLMs includes that of determining the right proportion of each value to apply when formulating a response to a user request or prompt.

How, then, can a "win" in ethics be defined for the purposes of reinforcement learning within the context of LLMs? Given the ambiguity of ethical criteria as well as the general incompatibility between the values of helpfulness, honesty and harmlessness, how can a precise goal or objective be defined by which to train LLMs to act more ethically?

This problem remained a barrier to the adoption of LLMs until a special technique was developed that enabled reinforcement learning to be applied to more "insightful" tasks based solely on human judgement, such as ethics. This technique came to be known as "reinforcement learning from human feedback" (RLHF).[11]

How it works is that, instead of attempting to programmatically define a set of ethical criteria directly, RLHF leverages the capabilities of machine learning to indirectly "discover" the features of such criteria by modeling the preferences of human evaluators. In general, the technique follows a five-step process:

---

[10] See *Aristotle*, Nicomachean Ethics, 1140b8.

[11] See *Christiano P., Leike J., Brown T. et al.*, Deep Reinforcement Learning from Human Preferences, 2017, <https://arxiv.org/abs/1706.03741> [25.11.2025]; *Ziegler D., Stiennon N., Wu J. et al.*, Fine-Tuning Language Models from Human Preferences, 2019, <https://arxiv.org/pdf/1909.08593.pdf> [25.11.2025]; and *Stiennon N., Ouyang L., Wu J. et al.*, Learning to summarize from human feedback, *34th Conference on Neural Information Processing Systems* (NeurIPS 2020), <https://proceedings.neurips.cc/paper/2020/file/1f89885d556929e98d3ef9b86448f951-Paper.pdf> [25.11.2025].

1. Task a group of human evaluators to review multiple LLM responses to the same prompt and then rank the responses in order of most to least ethical, that is, according to how well each response balances the values of helpfulness, honesty and harmlessness;
2. Create a supervised training dataset from the prompts, responses and human rankings, with the rankings serving as labels;
3. Train a supervised model to learn the implicit features of what constitutes a "winning" response in the "game" of ethics, that is, what indirectly constitutes the criteria of the values of helpfulness, honesty and harmlessness;
4. Set this learned "preference model" as the reward function for the LLM within the context of a reinforcement learning environment; and
5. Further fine-tune the LLM to act in accordance with the values of helpfulness, honesty and harmlessness by rewarding it for responses that fit the criteria of the preference model and punishing it for responses that do not.

Despite RLHF's ability to define an ethical objective for use in reinforcement learning, its method for "automating ethics" comes with a number of limitations. The main drawback is that the technique cannot ensure that the judgements made by the human evaluators are in fact appropriate or ethical. Just because a group of randomly selected humans are tasked with using their judgement does not entail that the results are ethical. The evaluators themselves could be biased or prone to making flawed decisions, in which case RLHF would simply reinscribe the unethical tendencies of the evaluators, but under the guise of an "objective" mathematical process.

Moreover, even assuming a non-biased population of human evaluators, the conditions in which they exercise their judgement could be coercive or exploitative, thereby negatively affecting their ability to rank LLM responses appropriately. For example, as reported by *Time Magazine*, OpenAI used Kenyan workers paid less than $2 an hour to create their RLHF training data for ChatGPT.[12]

In response to concerns about RLHF, another technique was developed known as "reinforcement learning from AI feedback" (RLAIF).[13] This technique follows the same process as RLHF, but with two important differences: (1) instead of human evaluators, it tasks the LLM itself with evaluating multiple LLM responses to the same prompt; and (2) instead of a set of ethical values, it provides the LLM with a "constitution" consisting of a set of principles, along with some examples of appropriate evaluations. For this latter reason, RLAIF is sometimes referred to as "constitutional AI."

While RLAIF may improve the scalability of results, it still suffers from some of the same limitations as RLHF. Just as RLHF cannot ensure that the decisions made by a

[12] *Perrigo B.*, Open AI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic, *Time*, January 18, 2023, <https://time.com/6247678/openai-chatgpt-kenya-workers/> [25.11.2025].
[13] See *Bai Y., Kadavath S., Kundu S. et al.*, Constitution AI: Harmlessness from AI Feedback, December 2022, <https://arxiv.org/abs/2212.08073> [25.11.2025].

group of human evaluators are appropriate or ethical, so too RLAIF cannot guarantee that the LLM's evaluations are not biased or flawed in some way. Indeed, the risk may be even greater in the case of RLAIF, since the LLM is tasked with making ethical evaluations *before* it has been fine-tuned to act more ethically.

3. Risks to Data Protection and Privacy

LLMs carry with them significant privacy, data protection and data security risks, some of which may be mitigated and some of which may be inherent to the systems themselves. In this section, we set forth the various risks stemming from LLMs. Please note that LLMs present several risks that, while not as directly related to privacy and data security, deeply affect individuals and may fall under the consumer protection remit of DPAs (namely information manipulation, increased data processing, misinformation and disinformation). We discuss those harms as well at the end of this section.

3.1. Increased Data Processing

To address the perceived need for mass training data, many LLM developers set up systems that indiscriminately and continuously scrape the internet for data.[14] While some developers may review and "clean" the scraped data before use, like Google's C4, many either skip this step or cannot keep up quality checks without limiting the volume of information absorbed.[15] This means that training datasets may include inaccurate, biased, and discriminatory data as well as personal data of individuals completely unaware that their information is now being used by an LLM.

3.2. Loss of Data Rights

The nature of LLMs makes exercising certain data rights very challenging, particularly the right to correct data or request deletion of the personal data often present in training datasets. While some datasets may be more tightly curated and checked for the origin and necessity of including personal data, scraping datasets in particular may include unnecessary personal data, personal data that was only made available through data breaches, or defamatory or inaccurate information about an individual.

[14] See e.g. *Hines K.*, OpenAI Launces GPTBot With Details on How to Restrict Access, *Search Engine Journal*, Aug. 7, 2023, <https://www.searchenginejournal.com/openai-launches-gptbot-how-to-restrict-access/493394/> [25.11.2025]; *Schaul K. et al*., Inside the secret list of websites that make AI like ChatGPT sound smart, *Washington Post*, Apr. 19, 2023, <https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/> [25.11.2025].

[15] *Center for Countering Digital Hate*, Misinformation on Bard, Google's New AI Chat, April 5, 2023, <https://counterhate.com/research/misinformation-on-bard-google-ai-chat/> [25.11.2025].

3.2.1. Harassment, Impersonation and Extortion

LLM capabilities can be used for intentional abuse targeted at individuals. These forms of abuse often are crafted using the individual's personal data or generating false personal data that can be very challenging to disprove, impacting the individual's mental health, relationships, reputation and more.

3.2.2. Scams

Individuals can use LLMs to generate robo-texts, robo-emails and mailers, as well as using the text generated by LLMs in conjunction with audio and video synthetic content to create more persuasive impersonations. Not only does the sheer volume of scams put out increase, but LLMs can make the pool of people committing fraud exponentially larger by helping those with limited skills in a given language craft natural and believable-sounding content that would otherwise be more easily flagged as a scam.

3.3. Data Security Risks

Hackers and other bad actors can use LLMs to draft or scale up versions of malware code, phishing and spear-phishing attempts, and emails targeting businesses to gain account information or compromise email.[16] New threat methods specific to LLMs may also become a problem, such as mining information fed into the LLM's training dataset or strategically and purposely poisoning the dataset with bad data.

3.4. Bias

LLMs can easily perpetuate bias by including biased data in their training datasets, through algorithms that develop their own biases, and in outputs stemming from those biased training datasets and algorithms. While bias may be present in curated training datasets, there is a particularly high risk of bias where datasets are

[16] See, e.g., *SlashNext*, The State of Phishing 2023, *SlashNext Security*, Oct. 2023, <https://slashnext.com/state-of-phishing-2023/> [25.11.2025]; *Groll E.*, ChatGPT Shows Promise of Using AI to Write Malware*, CyberScoop*, December 6, 2022, <https://cyberscoop.com/chatgpt-ai-malware/> [25.11.2025]; *Hassold C.*, Executive Impersonation Attacks Targeting Companies Worldwide, *Abnormal Blog*, February 16, 2023, <https://abnormalsecurity.com/blog/midnight-hedgehog-mandarin-capybara-multilingual-executive-impersonation> [25.11.2025]; *Center for Strategic and International Studies*, A Conversation on Cybersecurity with NSA's Rob Joyce*, YouTube*, April 11, 2023, <https://youtu.be/MMNHNjKp4Gs?t=530> [25.11.2025]. (8:50 mark).

built from web scraping methods that bring in massive collections of data on a continuous basis. In these cases, the training datasets constantly expand and they are often not regularly checked for accuracy, bias, appropriateness for use, and other key metrics.

3.5. Disinformation

LLMs facilitate a higher volume of persuasive disinformation generation that can then be spread easily, cheaply, and at a much higher speed. The potential impact of this on elections, politics, news (particularly related to health or safety), and other highly sensitive areas is significant.

3.6. Misinformation/Hallucinations

Misinformation raises many of the same problems as disinformation with one important distinction – individuals spreading misinformation may genuinely believe what they are sharing is accurate. Misinformation can be generated from the input parameters supplied by the user or from inaccurate information generated by the LLM itself.

In general, there are two kinds of hallucinations. The first and more obvious kind are hallucinations triggered from prompts that unintentionally include false or misleading content. This is what happened with Meta's now defunct "Galactica" LLM. Originally marketed as a tool to aid in the production of "scientific knowledge,"[17] Galactica was taken offline after only three days after it was discovered it would produce scientific-sounding, but entirely false wiki articles on fictitious topics such as the "flux capacitor" or "Streep-Seinfeld theorem."[18]

The second kind of hallucination are those that arise directly from the LLM itself, unbeknownst to the user. These are more pernicious and difficult to detect. There are many documented examples,[19] but one notorious case involves false criminal accusations against an individual. After being asked "What scandals have involved law professors?" ChatGPT provided a false narrative claiming that a real-life law professor had been accused of sexual harassment by a student.[20] What is even more concerning, however, is that the prompt included a request to "[p]lease cite and quote newspaper

[17] See *Taylor R., Kardas M., Cucurell G. et al.*, Galactica: A Large Language Model for Science, 2022, <https://arxiv.org/abs/2211.09085> [25.11.2025].

[18] See *Davis E. and Sundstrom A.*, Experiment with GALACTICA, 2022, <https://cs.nyu.edu/~davise/papers/ExperimentWithGalactica.html> [25.11.2025].

[19] See *Marcus G. and Davis E.*, Large Language Models like ChatGPT say The Darnedest Things, 2023, <https://garymarcus.substack.com/p/large-language-models-like-chatgpt> [25.11.2025].

[20] See *Volokh E.*, Large Libel Models: ChatGPT-3.5 Erroneously Reporting Supposed Felony Pleas, Complete with Made-Up Media Quotes?, *Reason*, 2023, <https://reason.com/volokh/2023/03/17/large-libel-models-chatgpt-4-erroneously-reporting-supposed-felony-pleas-complete-with-made-up-media-quotes/> [25.11.2025].

articles," to which ChatGPT "helpfully" obliged by appending a false quote from a non-existent source.

4. Privacy Principles and Technical Mitigations

The core data protection and privacy risks of LLMs are not particularly novel. What primarily differentiates LLMs, and generative AI more broadly, from other forms of AI is the increase in scale of the data being processed, the complexity of the techniques used to develop and deploy the models, and the unprecedented scale and pace of adoption across the economy.

In this section, we discuss the application of privacy principles to LLMs as well as technical mitigations to the data protection and privacy risks associated with generative AI.

4.1. Privacy Principles

4.1.1. Lawful Basis

The developers and deployers of generative AI systems that process personal data must have a valid lawful basis under data protection and privacy legislation, and also be lawful in accordance with other applicable legislation (e.g. copyright law). For example, Article 6 of the GDPR offers six lawful bases, with additional requirements under Article 9 for special category data.

In terms of training data for generative AI, it is crucial to note that personal data that is publicly accessible still falls under data protection and privacy legislation in most jurisdictions, as stressed in a recent joint statement by the GPA's International Enforcement Cooperation Working Group (IEWG).[21] Apart from data protection, upcoming copyright rulings in US federal courts and in the UK[22] may carry significant weight in relation to the lawfulness principle within the GDPR if it is deemed that web-scraped training data violates copyright and intellectual property laws. DPAs, of course, rely on these rulings as it is beyond their remit to make these judgements themselves.

[21] *Global Privacy Assembly (GPA) International Enforcement Cooperation Working Group*, Joint statement on data scraping and the protection of privacy, August 2023, <https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf> [25.11.2025].

[22] *David E.*, Getty lawsuit against Stability AI to go to trial in the UK, *The Verge*, December 4, 2023, <https://www.theverge.com/2023/12/4/23988403/getty-lawsuit-stability-ai-copyright-infringement> [25.11.2025].

4.1.2. Purpose Limitation

The developers and deployers of LLMs and generative AI systems that process personal data need to ensure that this data is processed for specified explicit and legitimate purposes. Furthermore, they need to ensure that they do not process it beyond individuals' reasonable expectations, or for incompatible purposes.

4.1.3. Data Minimization

The developers and deployers of LLMs and other generative AI systems that process personal data should limit processing to what is "necessary" for their purpose. The greater the volume of personal data being processed, the greater the potential privacy risks and other harms to individuals there are.

Limiting the occurrence or processing of any personal information as early as possible is an important step towards protecting the rights of data subjects. To this end, developers should strive to apply data minimization to any occurrences of personal information in their data sets. A common approach is to apply data sanitation by exclusion and different anonymisation procedures. However, even with these techniques applied, it can be challenging to fully ensure that datasets do not contain any personal information. In cases where pre-collected third-party datasets are used for training, it is equally important to remove personal information in post-processing steps.

4.1.4. Transparency

The developers and deployers of LLMs and other generative AI systems that process personal data must implement transparency measures, and must do so particularly in relation to data subjects, who have a number of information rights. This should include information on what, how, when, and why personal data is collected and used in the process of training the system, including the sources of training data, the pre- and post-processing measures to remove personal information and the reliability of the prediction of the generated text.

4.1.5. Security

The developers and deployers of LLMs and other generative AI systems that process personal data must implement security measures. This is multifaceted. Personal data needs to be kept secure during storage, development, but also during

post-deployment to account for complex security issues such as prompt injection attacks, model inversion attacks,[23] and data leakages.

4.1.6. Accountability

The developers and deployers of LLMs and other generative AI systems that process personal data should ensure they can demonstrate compliance with data protection. Accountability is in effect a meta-principle that acts as a guarantor.

4.1.7. Accuracy

The developers and deployers of LLMs and other generative AI systems must ensure that any personal data processed by them is as accurate, complete, and up-to-date as is necessary for purposes for which it is to be used. This applies in particular to personal data used to train LLMs or generative AI models.

To support this principle, developers and deployers should have a process by which their LLM or generative AI system can be updated (for instance, by refining or retraining the model) in cases where inaccurate or out-of-date model inputs, such as training data, are discovered. In addition, developers and deployers should inform end-users about any known issues or limitations with the accuracy of model outputs. This may include where the training data is timebounded (i.e. only contains information up to a certain date); where the content may be adversely affected by non-representative sources; or where there are particular subject matters or prompts that tend to lead to inaccurate outputs.

4.1.8. Data Subject Rights

The rights of data subjects are at the core of data protection. The developers and deployers of LLMs and other generative AI systems that process personal data are fundamentally required to ensure that individuals can access, rectify, erase, and opt-out of the use of their data, among other rights. This is especially important in relation to special category data and respecting the rights of children.

[23] *Veale M., Binns R. and Edwards L.*, Algorithms that remember: model inversion attacks and data protection law, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, October 2018, <https://doi.org/10.1098/rsta.2018.0083> [25.11.2025].

4.2. Technical Mitigations

When it comes to training LLMs, there are multiple stages and types of technical interventions that one can make to mitigate privacy risk. In this section we will focus on what are the benefits and drawbacks of leveraging some of these interventions.

4.2.1. Curation and Pre-Processing

LLMs are trained on large amounts of text data and, given their capacity for memorization,[24] it is important to treat the models with the same risk-appropriate considerations that one would treat the data used to train it. In the process of collecting and curating the datasets, it is possible to make decisions and take steps to reduce the risk that the data used in training will violate people's privacy.

Source curation: An initial consideration is what type of data is being used to train[25] these models, with a focus on the original intended audience when the data was shared. One simple distinction is whether the data is private data, with this type of data carrying a clear privacy impact when it is used as part of the training process without consideration to the data subject's desires. However, a less often considered distinction is publicly accessible vs public (or open data). While all public (or open) data is publicly accessible, not all publicly accessible data should be treated as if it is public. Here, the distinction lies in the intent and expectations behind making that data available: public data refers to data that was crafted with the intent of being widely shared and used, for example, government datasets and or Wikipedia contributions, whereas some publicly accessible data may have been shared with the intent of being used and consumed in specific contexts, for example social media posts and product reviews. Research has shown that, even in the context of academic research, social media users may not feel comfortable having their data used without their consent[26] even if it is publicly accessible. To reduce the privacy risk of these models, it is important to obtain data from sources where the privacy expectations for data use from those associated with the content are in alignment with the intended goal of training an LLM.

Pre-processing (removing sensitive data): After datasets have been initially compiled, the next step involves the pre-processing of that data before it is used to train models. At this stage, one can leverage automated tools to detect and remove sensitive information, for example personal information, health information, and information surrounding sensitive topics like sexuality and religion. These tools can range from simply detecting the presence of this information and flagging it for human

[24] *Carlini N., Tramer F., Wallace E. et al.*, Extracting Training Data from Large Language Models, *30th USENIX Security Symposium (USENIX Security 21)*, 2633–2650, <https://arxiv.org/abs/2012.07805> [25.11.2025].
[25] "Train" used here encompasses both initial training and any fine tuning or additional training steps.
[26] *Fiesler C. and Proferes N.*, 'Participant' Perceptions of Twitter Research Ethics, *Social Media + Society,* Vol. 4(1), 2018, <https://doi.org/10.1177/2056305118763366> [25.11.2025].

review, to automatically removing, replacing, or obfuscating the information (for example, replacing all addresses to 123 Main St).

4.2.2. Differential Privacy

When training LLMs, it is possible to leverage privacy enhancing technologies such as differential privacy (DP),[27] to train models that are provably private. This can be done at different stages (e.g., training data, model training, model outputs), with different units of consideration (e.g., instance-level, group-level), and in different conditions (e.g., central, local, distributed). Each of these have unique considerations, benefits, and costs that we will discuss in this section. For a more comprehensive presentation of the different approaches, their implementations and considerations, we refer the reader to "How to DP-Fy ML."[28]

Unit of privacy: Defining the appropriate unit of privacy for differential privacy is critical in ensuring the developers are providing the privacy guarantees at the appropriate level, as it determines what will make two datasets be considered "neighboring" in the definition of differential privacy. Instance-level DP will provide protections for each sample included in the dataset, whereas group-level DP will provide protections at a higher level of abstraction (e.g., user-level, document-level, etc). For LLMs, it may be better to use group-level DP as the desired sequence-length used in the training of these models will not only impact model performance but will also impact the privacy guarantees and disentangling these two factors may be more beneficial. Furthermore, the high chance for repetition of instances at the instance-level will likely significantly dilute the privacy guarantees being provided. However, it is still important to carefully consider at which level of grouping it makes sense to define the unit of privacy. For example, while one might want to provide user-level DP, given that the training data frequently used to train these models are publicly accessible text from the internet, it may be impossible to do so as one cannot identify which samples were contributed by which users.

Implementation stage: There are multiple levels of granularity related to when one can implement DP. For the sake of simplicity this subsection will only address it at the level of model training. Applying DP at the stage of model training provides guarantees that an adversary would not be able to differentiate between models that

[27] The definition of differential privacy that is being used in this section is the one proposed in *Dwork C., McSherry F., Nissim K., Smith A.*, Calibrating noise to sensitivity in private data analysis, *Procedures of the Third Conference on Theory of Cryptography (TCC)*, 265–284, <http://dx.doi.org/10.1007/11681878_14> [25.11.2025]:

> We say that two datasets D and D′ are neighbors if they differ in exactly one record; more precisely, one dataset is a copy of the other but with a single record added or removed. Let ε be a positive scalar. A mechanism A guarantees ε-differential privacy if for any two neighboring datasets D and D′ , and for any S ⊆ Range(A),
>
> $$P[A(D) \in S] \leq \exp(\varepsilon) \times P[A(D') \in S]$$

[28] *Ponomareva N., Vassilvitskii S., Xu Z. et al.*, How to DP-fy ML: A Practical Tutorial to Machine Learning with Differential Privacy, Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23), 2023, 5823–5824, <https://arxiv.org/abs/2303.00654> [25.11.2025].

include or do not include a particular instance in the training data. The approaches that are most feasible for language models relate to gradient noise injecting, with differentially private stochastic gradient descent (DP-SGD) being the most used algorithm. We strongly recommend that those interested in implementing differential privacy when implementing their models engage with experts on this topic or, at a minimum, leverage available resources.[29]

4.2.3. Post-Processing and Machine Unlearning

An post-processing approach that has gained traction recently is called "machine unlearning," which is focused on being able to effectively modify already trained models so they can "forget" specific pieces of training data without resorting to a complete "naïve" retraining of the model from scratch. Current research into machine unlearning focusses on two main approaches: "exact" unlearning and "approximate" unlearning.[30]

- Exact unlearning aims to fully remove the influence of targeted training data points from the LLM by initially splitting the training data into multiple subsets and then training the LLM as an ensemble of sub-models. When data points are identified for removal, only the sub-model associated with the identified data points needs to be retrained.[31] This accelerates the process of retraining, which would otherwise be a slow and costly procedure.
- Approximate unlearning, on the other hand, focuses on the model itself. Instead of re-training with altered data, it adjusts model weights after the fact to attempt to reduce the influence of targeted training data points. While its removal of information is less precise than exact unlearning, approximate unlearning may be less complex and costly in certain cases.

While proponents of machine unlearning say an effective approach—should it be developed—could improve privacy and help remove the influence of inaccurate or outdated data, truly deleting requested data cannot simply be done by erasing it from a database: the data's *influence*—such as the effect it has on a model's weights—must also be removed from machine learning models and other artifacts that exist downstream from where a requester's information is stored. Furthermore, as mentioned above, recent research has pointed out that removing specific instances of data from a model's training data can expose previously safe data.[32] For now, this area of research remains too nascent and without a clear answer on how effective "machine

[29] For example, ibid.

[30] See *Xu J., Wu Z., Wang C., Jia X.*, Machine Unlearning: Solutions and Challenges, 2024, <https://arxiv.org/abs/2308.07061> [25.11.2025].

[31] See *Yan H., Li X., Guo Z. et al.*, ARCANE: An Efficient Architecture for Exact Machine Unlearning, 2022, <https://www.ijcai.org/proceedings/2022/0556.pdf> [25.11.2025].

[32] See *Carlini et al.*, *supra* note 25.

unlearning" will be. Respecting data subject rights in the development and deployment of LLMs continues to raise challenges.[33]

5. Conclusion

The questions surrounding LLMs have recently coalesced to form one of the most challenging areas of engagement on the part of DPAs. Not only is the technology itself complex, with unique details and additional stages of development in comparison to other AI systems; LLMs raise various privacy and data protection risks whose understanding and appropriate redress depends fundamentally on an effective grasp of the underlying workings of the technology.

In this paper, we have attempted to provide an in-depth, multifaceted analysis of LLMs from the point of view of privacy and data protection, with a view towards better positioning DPAs to face the challenges posed by LLMs. The work of DPAs is only beginning with respect to LLMs and related generative AI technologies. As the field of generative AI continues to advance, it is expected that the challenges will continue to grow as well.

[33] *Zhang D., Finckenberg-Broman P., Hoang T. et al.*, Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions, *Algorithms that forget: Machine unlearning and the right to erasure, 2023,* <https://arxiv.org/pdf/2307.03941> [25.11.2025].

Bibliography:

1. *Askell A., Bai Y., Chen A. et al.*, A General Language Assistant as a Laboratory for Alignment, 2021, <https://doi.org/10.48550/arXiv.2112.00861> [25.11.2025].
2. *Aristotle*, *Nicomachean Ethics*, 1140b8.
3. *Bai Y., Kadavath S., Kundu S. et al.*, Constitution AI: Harmlessness from AI Feedback, December 2022, <https://arxiv.org/abs/2212.08073> [25.11.2025].
4. *Bommasani R., Hudson D., Adeli E. et al.*, On the Opportunities and Risks of Foundation Models, August 2021, <https://doi.org/10.48550/arXiv.2108.07258> [25.11.2025].
5. *Carlini N., Tramer F., Wallace E. et al.*, Extracting Training Data from Large Language Models, *30th USENIX Security Symposium (USENIX Security 21)*, 2633–2650, <https://arxiv.org/abs/2012.07805> [25.11.2025].
6. *Center for Countering Digital Hate*, Misinformation on Bard, Google's New AI Chat, April 5, 2023, <https://counterhate.com/research/misinformation-on-bard-google-ai-chat/> [25.11.2025].
7. *Center for Strategic and International Studies*, A Conversation on Cybersecurity with NSA's Rob Joyce*, YouTube*, April 11, 2023, <https://youtu.be/MMNHNjKp4Gs?t=530> [25.11.2025].
8. *Christiano P., Leike J., Brown T. et al.*, Deep Reinforcement Learning from Human Preferences, 2017, <https://arxiv.org/abs/1706.03741> [25.11.2025].
9. *Davis E. and Sundstrom A.*, Experiment with GALACTICA, 2022, <https://cs.nyu.edu/~davise/papers/ExperimentWithGalactica.html> [25.11.2025].
10. *David E.*, Getty lawsuit against Stability AI to go to trial in the UK, *The Verge*, December 4, 2023, <https://www.theverge.com/2023/12/4/23988403/getty-lawsuit-stability-ai-copyright-infringement> [25.11.2025].
11. *Dwork C., McSherry F., Nissim K. and Smith A.*, Calibrating noise to sensitivity in private data analysis, Procedures of the Third Conference on Theory of Cryptography (TCC), 265–284, <http://dx.doi.org/10.1007/11681878_14> [25.11.2025].
12. *Fiesler C. and Proferes N.*, 'Participant' Perceptions of Twitter Research Ethics, *Social Media + Society,* Vol. 4(1), 2018, <https://doi.org/10.1177/2056305118763366> [25.11.2025].
13. *Global Privacy Assembly (GPA) International Enforcement Cooperation Working Group*, Joint statement on data scraping and the protection of privacy, August 2023, <https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf> [25.11.2025].
14. *Groll E.*, ChatGPT Shows Promise of Using AI to Write Malware*, CyberScoop*, December 6, 2022, <https://cyberscoop.com/chatgpt-ai-malware/> [25.11.2025].
15. *Hassold C.*, Executive Impersonation Attacks Targeting Companies Worldwide, *Abnormal Blog*, February 16, 2023,

<https://abnormalsecurity.com/blog/midnight-hedgehog-mandarin-capybara-multilingual-executive-impersonation> [25.11.2025].

16. *Hines K.*, OpenAI Launces GPTBot with Details on How to Restrict Access, Search Engine Journal, Aug. 7, 2023, <https://www.searchenginejournal.com/openai-launches-gptbot-how-to-restrict-access/493394/> [25.11.2025].
17. *IWGDPT*, Working Paper on Large Language Models (LLMs), December 27, 2024, <https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20241206-WP-LLMs.pdf?__blob=publicationFile&v=2> [25.11.2025].
18. *Karpathy A.*, Let's build GPT: from scratch, in code, spelled out, January 2023, <https://www.youtube.com/watch?v=kCc8FmEb1nY> [25.11.2025].
19. *Knight W.*, A Stanford Proposal over AI's 'Foundations' Ignites Debate, *Wired*, September 2021, <https://www.wired.com/story/stanford-proposal-ai-foundations-ignites-debate/> [25.11.2025].
20. *Khandelwal U., Clark K., Jurafsky D. et al.*, Sample Efficient Text-Summarization Using a Single Pre-Trained Transformer, 2019, <https://doi.org/10.48550/arXiv.1905.08836> [25.11.2025].
21. *Marcus G. and Davis E.*, Large Language Models like ChatGPT say The Darnedest Things, 2023, <https://garymarcus.substack.com/p/large-language-models-like-chatgpt> [25.11.2025].
22. *Perrigo B.*, Open AI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic, *Time*, January 18, 2023, <https://time.com/6247678/openai-chatgpt-kenya-workers/> [25.11.2025].
23. *Ponomareva N., Vassilvitskii S., Xu Z. et al.*, How to DP-fy ML: A Practical Tutorial to Machine Learning with Differential Privacy, *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23*), 2023, 5823–5824, <https://arxiv.org/abs/2303.00654> [25.11.2025].
24. *Schaul K. et al*., Inside the secret list of websites that make AI like ChatGPT sound smart, *Washington Post*, Apr. 19, 2023, <https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/> [25.11.2025].
25. *Silver D., Huang A., Maddison C. et al.*, Mastering the game of Go with deep neural networks and tree search, *Nature*, Vol. 529, 2016, 484–489, <https://doi.org/10.1038/nature16961> [25.11.2025].
26. *SlashNext*, The State of Phishing 2023, *SlashNext Security*, Oct. 2023, <https://slashnext.com/state-of-phishing-2023/> [25.11.2025].
27. *Stiennon N., Ouyang L., Wu J. et al.*, Learning to summarize from human feedback, *34th Conference on Neural Information Processing Systems* (NeurIPS 2020), <https://proceedings.neurips.cc/paper/2020/file/1f89885d556929e98d3ef9b86448f951-Paper.pdf> [25.11.2025].
28. *Taylor R., Kardas M., Cucurell G. et al.*, Galactica: A Large Language Model for Science, 2022, <https://arxiv.org/abs/2211.09085> [25.11.2025].

29. *Veale M., Binns R. and Edwards L.*, Algorithms that remember: model inversion attacks and data protection law, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, October 2018, <https://doi.org/10.1098/rsta.2018.0083> [25.11.2025].
30. *Vinyals O., Babuschkin I., Czarnecki W. et al.*, Grandmaster level in StarCraft II using multi-agent reinforcement learning, Nature, vol. 575, 2019, 350–354, <https://doi.org/10.1038/s41586-019-1724-z> [25.11.2025].
31. *Volokh E.*, Large Libel Models: ChatGPT-3.5 Erroneously Reporting Supposed Felony Pleas, Complete with Made-Up Media Quotes? Reason, 2023.
32. *Xu J., Wu Z., Wang C. and Jia X.*, Machine Unlearning: Solutions and Challenges, 2024, <https://arxiv.org/abs/2308.07061> [25.11.2025].
33. *Yan H., Li X., Guo Z. et al.*, ARCANE: An Efficient Architecture for Exact Machine Unlearning, 2022, <https://www.ijcai.org/proceedings/2022/0556.pdf> [25.11.2025].
34. *Zhang D., Finckenberg-Broman P., Hoang T. et al.*, Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions, *Algorithms that forget: Machine unlearning and the right to erasure*, 2023, <https://arxiv.org/pdf/2307.03941> [25.11.2025].
35. *Ziegler D., Stiennon N., Wu J. et al.*, Fine-Tuning Language Models from Human Preferences, 2019, <https://arxiv.org/pdf/1909.08593.pdf> [25.11.2025].

Petru Emanuel Zlătescu*

Selected Aspects of International Cooperation under the New Swiss Federal Act on Data Protection**

The totally revised Swiss Federal Act on Data Protection (FADP) aims at strengthening the data protection of individuals in Switzerland, in particular through the alignment with the latest developments in data protection law at international level on the one hand, as well as through the adaptation to the latest technological developments on the other. This also extends to the enhancement of the powers of the Federal Data Protection and Information Commissioner (FDPIC). In addition to the consolidation of independence and autonomy from external instruction, the new FADP has also equipped the FDPIC with a range of new competencies in the domain of international cooperation. The cornerstones of this area are the international administrative assistance between data protection authorities and the direct delivery of documents abroad. The two legal concepts under discussion are both based fundamentally on the principle of reciprocity.

***Keywords**: Swiss Federal Data Protection and Information Commissioner, Swiss Federal Act on Data Protection, Administrative Assistance, International Cooperation, Direct Service of Documents.*

* Senior Lecturer and Researcher at the Law Faculty of the Fernuni University in Brig, Switzerland Deputy Head of the Directorate for International Affairs at The Swiss Federal Data Protection and Information Commissioner (FDPIC).

** The views expressed in this article are exclusively those of the author and do not in any way bind his employer. The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

1. The New Swiss Federal Act on Data Protection

The totally revised Swiss Federal Act on Data Protection (FADP) entered into force on the 1st of September 2023. It aims at strengthening data protection by improving the transparency of data processing and the control that data subjects have over their personal data. At the same time, the new law aims to increase the sense of responsibility of controllers, for example by requiring them to take data protection regulations into account when planning new data processing operations. Supervision of the application of and compliance with federal data protection standards is also to be improved. Finally, Switzerland's attractiveness on the global economic market is to be maintained and improved, in particular by facilitating the transfer of personal data to other countries or international organization and promoting the development of new economic sectors in the field of digitalisation of society, based on a high, internationally recognised standard of protection.

The international dimension of the new law played a pivotal role in the broader landscape against which this modern piece of privacy legislation was enacted. In addition to adapting to the latest technological developments, the primary reasons for the total revision of the FADP included the implementation of the latest international law requirements and the alignment with the most recent international standards.[1] The FADP has undergone extensive revisions with a view to implementing the international law obligations arising from Switzerland's Schengen association in the area of data protection (in particular, Regulation (EU) 680/2016 [LED][2]) and the requirements of Convention 108+ of the Council of Europe (CETS No. 223)[3], which Switzerland has ratified. It is also important to emphasise that the new FADP is intended to ensure that Swiss data protection law is equivalent to that of the EU and thus meets the EU's adequacy requirements under the GDPR[4].[5] Since 2000, Switzerland has already benefited from an adequacy decision by the EU under Directive 95/46/EC[6]. 2024, the European Commission confirmed the adequacy of the Swiss level of data protection in accordance with the GDPR.[7] Moreover, the new FADP

[1] *Epiney A., Zlătescu E P.,* Art. 1 FADP, in*: Bieri A., Powell J.,*(eds.), OFK DSG, Zurich 2023, note 4; see also *Frey N.,* Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, in: Jusletter 17. September 2018.

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119, 89.

[3] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 10 October 2018 (CETS No. 223).

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119, 1.

[5] *Epiney A., Frei N.,* Die völker- und europarechtliche Einbettung des DSG, in: *Bieri A., Powell J.*(eds.), OFK DSG, Zurich 2023, note 13 et seq.; see also *Wiewiórowski W*., Welcome Letter, Journal of Personal Data Protection Law 1/2023, 11.

[6] Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ 2000 L 215, 1.

[7] COM(2024) 7 final.

codifies numerous elements of the case law of the ECtHR and the Swiss Federal Supreme Court, and introduces, for example, the right to erasure (Art. 32 para. 2 FADP).

2. New Powers and Competences of the FDPIC

The new FADP brought significant changes with regard to the competences and powers of the Federal Data Protection and Information Commissioner (FDPIC). The Commissioner is now elected by Parliament, and his independence and freedom from instructions are guaranteed by federal act.[8] This institutional strengthening of the federal data protection authority can be traced back primarily to international law, in particular Regulation (EU) 680/2016 (LED), which is binding on Switzerland due to its Schengen association. The 2014 EU evaluation of Switzerland's compliance with Schengen requirements also stipulated that the Commissioner must be empowered to issue legally binding rulings.[9] Further reasons for strengthening the independence and powers of the Commissioner can also be derived from Articles 15 and 16 of the Council of Europe's Convention 108.

In addition to the above-mentioned points, it is notable that the fully revised FADP also endows the Commissioner with competencies that enable effective engagement in the realm of international cooperation with foreign data protection authorities.[10] This corresponds to the role of data protection supervisory authorities prescribed by Convention 108+, which devotes a whole chapter[11] to cooperation and mutual assistance between data protection authorities. Such cooperation is meant to enable data protection authorities to carry out their respective responsibilities under national law. The aim is to address the increasingly frequent cross-border constellations in which personal data of data subjects from one jurisdiction are processed in the territory of another state. Various provisions of the FADP provide for specific means that the FDPIC can employ in cross-border cases, both in relation to foreign data protection authorities and to controllers abroad. In view of advancing digitalisation and the associated processing of almost incalculable quantities of personal data by global technology companies that are not bound by geographical borders, cooperation between data protection supervisory authorities at international level is essential.[12]

[8] Art. 43 FADP.
[9] *Epiney A., Frei N.,* Die völker- und europarechtliche Einbettung des DSG, in: *Bieri A., Powell J.(eds.),* OFK DSG, Zurich 2023, note 8.
[10] Art. 58 para. 1 let. b FADP.
[11] Chapter V Convention 108+ (CETS No. 223).
[12] *Kerbosas C., Lennman C.,* in: *Meier P., Métille S.,* (eds.), Loi fédérale sur la protection des données, Basel 2023, Art. 55 N 1 *et seq*..

Consequently, Art. 58 para. 1 let. b FADP stipulates that the FDPIC shall cooperate with foreign authorities in charge of data protection. More specifically, Art. 55 FADP empowers the Commissioner to engage in administrative assistance with foreign data protection authorities in accordance with the principle of reciprocity, and Art. 58 para. 3 FADP entails the competence of the FDPIC to declare to foreign data protection supervisory authorities that direct service of their official documents is permissible in the field of data protection in Switzerland, provided that Switzerland is granted reciprocal treatment. As is clear from the relevant provisions of the FADP, ensuring mutuality is the cornerstone and central prerequisite for the various forms of cooperation between the FDPIC and its counterparts from other jurisdictions. In addition, Switzerland is obliged under international law to cooperate and provide mutual assistance between data protection authorities: generally, under Art. 16 *et seq*. of Convention 108+) of the Council of Europe and, in the area of criminal prosecution, under Art. 46 para. 1 let. H and Art. 50 of Directive (EU) 680/2016 (LED).

3. Administrative Assistance

3.1. General Remarks

Administrative assistance refers to the exchange of information and personal data between the FDPIC and foreign data protection authorities in a concrete case for the purpose of enabling the requesting data protection authority to fulfil its legal duties and competencies.[13] In implementation of Article 17 of Convention 108+ and Article 50 of Directive (EU) 2016/860, Article 55 regulates mutual assistance between data protection authorities at international level.[14] As stated in Article 17 of Convention 108+, data protection authorities are bound by a duty of cooperation, to the extent that is necessary for the fulfilment of their statutory tasks and powers.[15] The FADP conclusively regulates the conditions under which the FDPIC can engage in administrative assistance with foreign data protection authorities. A competence of the Commissioner which was discussed during the legislative process and which would have authorised him to regulate the modalities of cooperation with his foreign counterparts through the conclusion of public international law agreements was not included in the law.[16] However, this competence is delegated by the FADP to the Federal Council, which, pursuant to Art. 67 FADP, may conclude international treaties in the field of data protection. Such international agreements may also regulate cooperation between data protection authorities.

[13] *Baeriswyl B., in: Baeriswyl B.,* et al. (eds.), Datenschutzgesetz, Berne 2023, Art. 55 N 5; *Rosenthal D.,* Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, note 190.

[14] *Kerbosas C.*, *Lennman C.,* in: *Meier P.*, *Métille S.*(eds.), Loi fédérale sur la protection des données, Basel 2023, Art. 55 N 7.

[15] See: CÉCILE DE TERWAGNE, La nouvelle loi suisse de protection des données dans le contexte international, in *Epiney A., Moser S., Rovelli S.,* (eds.), Die revision des Datenschutzgesetzes des Bundes, Zurich 2022, 47, 86.

[16] Federal Council, Message accompanying the totally revised FADP, 7104.

It should be emphasized that, within the scope of application of Art. 55 of the FADP, the FDPIC is in principle not obliged to engage in administrative assistance. This discretionary provision gives the Commissioner the power to decide whether and when to engage in administrative assistance. For instance, the FDPIC can decline a request for administrative assistance if the law of the requesting data protection authority does not guarantee an adequate level of data protection within the meaning of Art. 16 FADP.[17]

Despite the wording of Art. 55 para. 1 FADP, stricter rules on mutual assistance between data protection authorities apply in law enforcement matters between Schengen states. For example, under Art. 50 LED[18], the FDPIC is obliged to provide mutual assistance to the data protection authorities of other Schengen states. Data protection authorities must provide each other with relevant information and mutual assistance to implement and apply the LED consistently, and to establish effective cooperation measures. This assistance covers information requests and supervisory measures, such as requests to carry out consultations, inspections and investigations. Under the scope of the LED, the Commissioner is required to reply to a request from another supervisory authority from the Schengen area without undue delay, and in any case no later than one month after receiving the request.

3.1.1. Conditions

3.1.1.1. Reciprocity

Article 55 FADP has established a number of five cumulative conditions that must be met in order for the FDPIC to engage in administrative assistance. As highlighted above, the first and most relevant of these in practice is the requirement of reciprocity. Notwithstanding the view held by part of the doctrine,[19] neither the wording of Art. 55 FADP nor the materials arising from the legislative process leading to the enactment of the Act indicate that there are any formal requirements, such as the conclusion of an international agreement, nor is there a prescribed minimum content that must be stipulated.

3.1.1.2. Purpose Limitation

An essential feature of administrative assistance is that the information and personal data exchanged by the data protection authorities involved are used exclusively for the specific proceedings for which administrative assistance was requested, in accordance with the principle of specialty. The FDPIC must therefore

[17] Federal Council, Message accompanying the totally revised FADP, 7095.
[18] See also Art. 349a et seq. Swiss Criminal Code.
[19] *Baeriswyl B.,* in*: Baeriswyl B.,* et al. (eds.), Datenschutzgesetz, Berne 2023, Art. 55 note 6.

ensure that this purpose limitation is guaranteed by the recipient data protection authority. The importance of the purpose limitation principle is also reflected by Article 19 of Convention 108+, according to which a data protection authority which has received information from one of its foreign counterparts, either accompanying a request or in reply to its own request, shall not use that information for purposes other than those specified in the request.

3.1.1.3. Professional, Business and Manufacturing Secrets

A further condition for engaging in administrative assistance is the obligation of the recipient authority to comply with professional, business and manufacturing secrets contained in the information received in the context of administrative assistance. If such secrets are contained in the information transmitted, the FDPIC is required to inform the parties concerned before transmitting the information to the foreign authority and to invite them to submit their observations, provided that this is not impossible or would cause disproportionate effort. In practice, this requirement could have limited scope, as for instance according to Art. 50 para. 2 FADP, professional secrets are in principle excluded from the information to be made available to the FDPIC in the context of an investigation.

3.1.1.4. Disclosure to Third Parties

The disclosure of the information and personal data transmitted by the receiving authority to third parties requires the prior approval of the data protection authority that transmitted the data.

3.1.1.5. Conditions or Restrictions

The FADP also allows the transmitting data protection authority to impose conditions or restrictions on the receiving authority with regard to the personal data and information transmitted. Examples of possible conditions identified by the doctrine include requirements for the anonymisation of personal data, the setting of a specific time limit within which the personal data must be deleted by the receiving authority, or the condition that information and personal data may only be transferred if the FDPIC is also informed of the results of the investigation abroad.[20]

3.1.2. The Object of Administrative Assistance

With regard to personal data and information that the FDPIC may exchange with its counterpart supervisory authorities within the scope of administrative assistance,

[20] *Baeriswyl B., in: Baeriswyl B.,* et al. (eds.), Datenschutzgesetz, Berne 2023, Art. 55 note 11.

the FADP provides a non-exhaustive list. This includes, in particular, the identity of the controller and the processor, the personal data processed, the purpose of the processing, the recipient or the identity of the data subject. The latter may only be disclosed either if the data subject has given their consent or if this is essential for the performance of a legal task of one of the data protection authorities involved.

4. The Direct Service of Documents Abroad

4.1. General Considerations

Another significant element of novelty of the totally revised FADP in the field of international cooperation between supervisory authorities relates to the direct service of official documents by foreign data protection authorities. The service of an official document to a recipient abroad or from abroad in Switzerland constitutes, under Swiss law, an act of public authority, which cannot be performed on the territory of another State due to its territorial sovereignty. In general, such an act must either be carried out by the recipient's country of residence through a public international law treaty or be authorised by the other country. In the absence of authorisation, the direct notification of decisions, rulings, or other official documents abroad without first obtaining the consent of the State of residence of the addressee and without complying with the procedures established by the latter's law or by a bilateral or multilateral international treaty constitutes a violation of the sovereignty and independence of that State. If this is the case, the notification is, according to the case law of the Federal Court, absolutely null and void.[21]

Swiss legislation contains two legal bases that enable the service of foreign official documents in the field of data protection within Swiss territorial jurisdiction: Article 58 para. 3 FADP and the European Convention on the Service Abroad of Documents relating to Administrative Matters of 17 November 1977 (CETS No. 094).

4.2. Article 58 paragraph 3 FADP

In addition to the mutual assistance procedure in the strict sense regulated in Art. 55 FADP, the FDPIC may, pursuant to Art. 58 para. 3 FADP, allow foreign data protection authorities to transmit their rulings directly to Switzerland without violating Art. 271 of the Swiss Criminal Code. Direct service within the meaning of Art. 58 para. 3 FADP requires a general and abstract declaration by the Commissioner to a foreign data protection authority. It is not limited to a specific individual case or to a specific category of matters. As in Art. 55, Art. 58 para. 3 FADP presupposes reciprocal rights

[21] Swiss Federal Supreme Court, BGE 143 III 28 cons.2.2.1.

as a prerequisite for direct service. The service may be effected either by postal service or through the diplomatic or consular representation of the delivering State.[22]

According to the wording of Article 58 para. 3 FADP, direct notification may be authorised in general by the FDPIC if three cumulative conditions are met: direct notification is limited to the field of data protection from a Swiss perspective, the notification is made by an administrative authority charged specifically with data protection, and Switzerland is granted reciprocal rights. In addition to these conditions, part of the doctrine is of the opinion that it is necessary to balance the interests at stake, taking into account the potential consequences of authorisation on Switzerland's sovereignty and on the recipients of foreign official acts. Among the public interests, consideration should be given to respect for the rule of law (in particular the principles of legality and proportionality), foreign policy interests and the consequences of authorisation or refusal for Switzerland, particularly in terms of the economy and the protection of personal data. According to the same author, private interests should include respect for legally protected secrets, the availability of effective legal remedies in foreign proceedings, the existence of independent and impartial judicial review, economic interests, the interests of data subjects in the protection of their personal data and the adequacy of the State's data protection regime for the purposes of the authorisation.[23]

4.2.1. European Convention on the Service Abroad of Documents Relating to Administrative Matters

Ten member states of the Council of Europe[24] have ratified the Convention. Article 1 para. 1 of the Convention stipulates that the contracting states undertake to provide mutual assistance in the service of documents in administrative matters. In principle, the agreement applies to all administrative matters, except tax and criminal matters. In accordance with Article 1 para. 3, the parties may also exclude other areas of law. At the time of signing the Convention, Switzerland issued a declaratory statement indicating that the Convention's scope did not encompass financial market supervision or intelligence matters. Consequently, it can be deduced that the provisions of this Convention pertain to the realm of data protection. This assertion is substantiated by the absence of any explicit exclusion of data protection in Article 1 para 2 of the Convention, and the absence of any declaration by Switzerland that data protection is to be excluded from its ambit. In particular, the Convention provides for notification to be made via diplomatic or consular channels (Article 12), postal services (Article 11), consular officers or diplomatic agents of the requesting state (Article 10),

[22] *Cattaneo G.,* in: *Meier P., Métille S*., (eds.), Loi fédérale sur la protection des données, Basel 2023, Art. 58 note 79.
[23] *Cattaneo G., in: Meier P., Métille S.,* (eds.), Loi fédérale sur la protection des données, Basel 2023, Art. 58 note 79 et seq.
[24] For the status of ratifications, see: <https://www.coe.int/en/web/conventions/full-list2?module=signatures-by-treaty&treatynum=094> [24.7.2025].

or the Central Authority of the requested state (Article 2 et seq.). As a rule, pursuant to Art. 6 of the Convention, the requesting authority may forward the order to a central authority in the country where the service is to be carried out. This authority will then serve the document on the addressee and return the requesting authority a certificate of service. As set out in Article 2, paragraph 1 of the Convention, each Contracting State shall designate a central authority responsible for receiving requests for the service of documents in administrative matters from the authorities of other Contracting States, and for responding to such requests. Federal states may designate more than one central authority. Switzerland has issued a declaration stipulating that its central authority for the purposes of the Convention is the Federal Office of Justice.

The Convention obliges the state parties to provide mutual assistance in the service of documents in administrative matters.[25] According to the message of the Federal Council, the agreement is intended to facilitate cooperation in cases where there are no legal provisions governing mutual assistance. Even if Art. 55 FADP does not refer to the service of documents; it must be interpreted in accordance with international law and in the light of the agreement. The Convention must also be taken into account when applying Art. 58 para. 3 FADP.

Given the federal law through Article 58 para. 3 of the FADP does not comprehensively regulate the direct service of foreign official administrative documents in the field of data protection, but rather through a single general provision, it can be assumed that the FADP and the Convention are compatible, as both aim to strengthen the rapid and effective application and enforcement of data protection provisions. In any event, Art. 58, para. 3 of the FADP must be interpreted in accordance with international law. It should also be noted that the legislative materials do not suggest that the Federal Assembly intended to adopt a provision contrary to the Convention when it adopted Art. 58 para. 3 FADP during the total revision of the Act. The notification procedures set out in the Convention therefore apply to cases, where data protection authorities from countries that have ratified the convention seek the service of documents on the territory of Switzerland.

5. Conclusion

While the scale of cases data protection authorities face in their day-to-day practice can be formidable, the procedural aspects they manage play an equally crucial role in shaping the outcomes of their efforts. In the context of the international dimension of Switzerland's Federal Data Protection Act, procedural considerations come to the forefront. Topics such as administrative assistance between data protection authorities or the direct service of their documents abroad illustrate the complex processes involved in international collaboration. These elements underscore

[25] Federal Gazette, 2017 5957.

the importance of efficient coordination to navigate major cases effectively. Various provisions of the FADP provide for specific means that the FDPIC can employ in cross-border cases, both in relation to foreign data protection authorities and to controllers abroad. Within the domain of these forms of international cooperation, the legally binding guarantee of reciprocity assumes a pivotal role.

Bibliography:

1. *Bieri A., Powell J. (*eds.), OFK DSG – Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zurich 2023.
2. *Epiney A., Moser S., Rovelli S.,* (eds.), Die Revision des Datenschutzgesetzes des Bundes, Zurich 2022.
3. *Baeriswyl B.* et al. (eds.), Datenschutzgesetz, Berne 2023.
4. Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ 2000 L 215, 1.
5. European Convention on the Service Abroad of Documents relating to Administrative Matters of 17 November 1977 (CETS No. 094).
6. *Rosenthal D.,* Das neue Datenschutzgesetz, in: Jusletter 16. November 2020
7. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119, 89.
8. *Frei N.,* Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, in: Jusletter 17. September 2018.
9. *Meier P., Métille S. (*eds.), Loi fédérale sur la protection des données, Basel 2023.
10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119, 1.
11. Swiss Federal Council, Message accompanying the total revision of the Federal Act on Data Protection and on the amendment of further normative acts in the field of data protection of 15 September 2017, OJ 2017 9641.
12. *Wiewiórowski W*., Welcome Letter, Journal of Personal Data Protection Law 1/2023, 11.

Rachel Masterton*

International Cooperation: Expanding Capacity, Amplifying Impact**

The processing of personal data is often on a global scale with global impacts. Regulation, on the other hand, has been constructed according to geographical boundaries. International cooperation can be the resolution to those geographical differences and by engaging with the four modalities of regulation identified by Lawrence Lessig[1] in his 'Pathetic Dot Model' this cooperation can serve to expand the capacity and amplify the impact of data protection and privacy authorities.

Keywords: *Lessig, Pathetic Dot Model, data protection, international cooperation, regulation, privacy.*

1. Introduction

Personal data has become a global business stretching beyond geographical boundaries. The regulation of those entities making money from personal data, however, remains firmly anchored to these traditional, jurisdictional boundaries. Even when legislation is shared by a number of countries, such as the European Union's General Data Protection Regulation[2], each jurisdiction has their own body tasked with regulation and enforcement, in some cases, several bodies.

International cooperation by data protection authorities is, therefore, vital to knit together disparate legal frameworks for a global response to global problems. However, there is more to be gained from international cooperation than simply smoothing out legal differences.

This paper seeks to explore the four modalities of regulation, as proposed by Lawrence Lessig[3] - law, societal norms, market and architecture - and, using case

* LLM, Deputy Data Protection Commissioner, Guernsey Data Protection Authority.

** The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

[1] *Lessig L., Code Version 2.0* (Basic Books 2006).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119.

[3] *Lessig L.*, Code and the Other Laws of Cyberspace, Basic Books, 1999.

studies, show how these modalities, when combined with international cooperation, can help data protection authorities expand their capacity and amplify their impact.

2. Understanding Lessig's Modalities of Regulation

Lawrence Lessig first wrote about the four modalities of regulation, also known as the 'Pathetic Dot Model' in his book 'Code and the Laws of Cyberspace'. He postulated that an entity ('the dot') is subject to four different forces that control or regulate its behaviour. These four forces are law, social norms, the market, and architecture, in Lessig's case, 'the code' underpinning cyberspace.

Law provides the rules that the State wants to control activity. It codifies what is right and what is wrong and provides mechanisms to judge the legality of activity and to sanction that which is deemed wrong. This informs the dot what is legal and what could happen if it does not follow the law.

Social norms are the unwritten rules of behaviour that operate within a society. They are not set by the State but rather by those people in the society to whom the social norms relate. Unless there is a crossover with a piece of legislation there are likely no formal sanctions imposed if a social norm is broken or ignored. However, the society itself will often act as the judge of the behaviour and make its feelings known in other ways. In days past, this would be by word of mouth. Now, in this digital age, social norms are the reason user-generated review platforms such as TripAdvisor hold so much power. They represent not what behaviour is legal or illegal but rather how someone felt the behaviour of a business met their expectations and a societal view of good or bad.

The market in which the dot operates has long been a way in which activity is regulated. Markets set prices based on supply and demand. A business can charge more for a rare product than it could for a more common one, even where a dispassionate view would suggest they are of the same value. Markets can also determine what an acceptable product or service is and those not meeting that standard can suffer by comparison.

Architecture relates to the physical and situational factors that act to constrain the dot. As Lessig puts it, architecture is "the way the world is, or the ways specific aspects of it are". Architecture shapes human behaviour, for example, the layout of a town controls or constrains how people interact with it. A person needs to follow the roads and move past the building rather than heading 'as the crow flies'.

The book Lessig wrote deals primarily with regulation of the cyberspace and was written in response to a commonly held belief that cyberspace could not be regulated. This therefore has some resonance in the data protection world and will be explored further later in this paper. However, it is clear from looking at the model, that the four modalities of regulation are not exclusive to the online world and can be considered in relation to the regulation of behaviour in other arenas. Lessig argues that these four modalities act on the dot, each individually but often simultaneously, to a greater or

lesser extent depending on the circumstance and that leveraging all modalities will have a greater impact than focusing solely on one.

As an example, one need look no further than the global initiative to combat climate change. Treaties have been signed[4] and legislation has been enacted[5] to curb emissions and remove some of the more harmful contributors of 'greenhouse gases' – regulation by law. Schools, colleges and third-sector bodies are educating people as to the difference they can make by changing behaviour and encouraging change in others – regulation by societal norms. Companies are making shifts in their production methods and creating new 'greener' products, shifting the market share away from more established but more harmful practises – regulation by the market. In addition, global reserves of non-renewable and harmful energy sources are depleting, forcing the world to think about alternative energy – regulation by architecture.

In the middle of those four modalities is the dot. Whether the dot in this example represents a person or a company, all four modalities are working on it, applying their pressure in their different ways, but all regulating the behaviour of the dot.

3. The Landscape of International Data Protection Regulation

As of 2 July 2025, 79% of the world's countries had some form of data protection or privacy legislation, according to statistics published by the United Nations Trade and Development ('UNCTAD')[6], with a further 3% of countries having draft legislation. Whilst these laws provide frameworks for the obtaining, use and storage of personal data, there is no overarching legal instrument that all 80% have signed up to and organisations with activities in several different jurisdictions will often find differences in the requirements and expectations of the regulators created by those laws. In some cases, such as in the United States of America, legislation is State-focused[7] or sector-focused[8] meaning different rules in different circumstances, even within the same country.

That said, there are two significant legal frameworks, the European Union's General Data Protection Regulations and the Council of Europe's Convention 108[9], that form the basis of many of the world's data protection and privacy legislation. There are many commonalities between these two frameworks. Both are built on

[4] Paris Agreement to the United Nations Framework Convention on Climate Change, adopted 12 December 2015, T.I.A.S. No. 16-110.

[5] Climate Change Act 2008 (c. 27).

[6] *UN Trade & Development*, 'Data Protection and Privacy Legislation Worldwide' <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

[7] The California Privacy Rights Act of 2020, implemented & enforced by the California Privacy Protection Agency <https://cppa.ca.gov/about_us/>.

[8] Health Insurance Portability and Accountability Act of 1996 (HIPAA) <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>.

[9] *Council of Europe*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 (opened for signature 28 January 1981).

fundamental principles; the processing of personal data must be lawful, fair and transparent, collected for specified legitimate purposes and not used beyond those purposes. Both frameworks provide individuals with rights over their personal data. These include the right to access personal data, to request rectification and erasure and the right to object to processing.

Both frameworks place an emphasis on accountability, requiring those using personal data to implement appropriate measures to ensure compliance and to be able to demonstrate that compliance. In addition, as both are designed to apply across jurisdictions, both frameworks contain provisions for international data transfers, to assist business in operating and to ensure that the safeguards provided by the frameworks travel with the personal data.

However, despite the broad similarities, even these two frameworks have significant differences. The GDPR is an EU regulation and as such is directly applicable in EU Member States. It is also detailed and prescriptive, leading to a robust framework that is the same across the EU and EEA. The GDPR provides a mechanism under which third countries can apply to have their own data protection legislation and regulatory frameworks determined as adequate. This assessment of the third country as essentially equivalent to the GDPR provides for the free-flow of personal data between EU and adequate jurisdictions without the additional safeguards a transfer outside the EU's boundaries would usually require. To date, 16 such decisions have been made.

The Convention 108 is, in contrast, an international treaty and whilst laying out guiding principles, is in no way as prescriptive as the GDPR. Signatory jurisdictions are required to enact their own domestic legal instruments to implement the principles of the Convention. As such, whilst its reach is wider than that of the GDPR, there can be differences in implementation across the 55 jurisdictions that have adopted it, 47 Member States of the Council of Europe and five non-European countries[10].

Whilst legislation may differ across the globe, cooperation between the regulators of different jurisdictions that have similar aims has long been an important part of the regulatory stage. In 1979, the first International Conference of Data Protection and Privacy Commissioners was held in Bonn, Germany[11]. Held in a different country each year (except for two 'at your desk' events during the COVID-19 pandemic) and hosted by a local data protection or privacy regulator, this conference has grown both in size and remit. Rebadged as Global Privacy Assembly[12] ("the GPA") and guided by an Executive Committee, supported by a secretariat, the GPA embraces the following as its vision: Consolidate the Global Privacy Assembly's leadership on personal data protection and privacy, maximizing its voice and influence across geographic and linguistic networks and strengthening the enforcement capacities of

[10] Council of Europe 'Chart of signatures and ratifications of Treaty 108'. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.

[11] Global Privacy Assembly 'History of the Assembly' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/>.

[12] Global Privacy Assembly <https://globalprivacyassembly.org/>.

authorities to move towards a higher level of global data protection and privacy that ensures effective protection of data subjects.[13]

As well as providing an annual forum for discussion between its over 130 members and observers, the GPA has adopted a plan[14] that articulates its strategic aims. These are focused around achieving a higher level of global data protection and privacy, maximising the voice and influence of the GPA and its members and strengthening enforcement capacities. To deliver on these aims, the GPA has a number of working groups[15] that bring together member data protection and privacy authorities that work in collaboration to achieve more than they could alone.

Of particular relevance to the theme of this paper is the International Enforcement and Cooperation Working Group[16]. Established as a permanent working group in 2019, the IEWG has the remit to "lay the foundations for the IEWG and GPA to facilitate practical enforcement cooperation"[17] with a particular focus on global issues that could affect people's data protection and privacy rights. It also seeks to develop and promote practical tools to assist international enforcement cooperation and to foster lines of communication with other relevant groups and privacy bodies to "coordinate and leverage opportunities"[18]. One tool supported by the IEWG is the Enforcement Cooperation Handbook[19] (the Handbook) that lays out ways in which authorities can work together to achieve common goals. The work of the IEWG and the Handbook will be discussed in the next section of this paper.

The Global Privacy Enforcement Network[20] (GPEN) was created in response to the OECD's Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy[21]. Paragraph 21 of that document called for the "establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders" to discuss cooperation and share best practices in dealing with cross-border issues. One of GPEN's headline initiatives is the annual 'Sweep', a mechanism "aimed at increasing awareness of privacy rights and responsibilities, encouraging compliance with privacy legislation, and enhancing cooperation between

[13] Global Privacy Assembly 'Mission and Vision' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision/>.
[14] Global Privacy Assembly 'Strategic Plan 2023 – 2025' <https://globalprivacyassembly.org/wp-content/uploads/2024/02/GPA-Strategic-Plan-final-version-update-oct10-1.pdf>.
[15] Global Privacy Assembly 'Working Group Reports' <https://globalprivacyassembly.org/document-archive/working-group-reports/>.
[16] Global Privacy Assembly 'International Enforcement Working Group Report – July 2024' <https://globalprivacyassembly.org/wp-content/uploads/2024/11/9.-IEWG-GPA-Annual-Report-2024.pdf>.
[17] Ibid.
[18] Ibid.
[19] Global Privacy Assembly 'An Enforcement Cooperation Handbook' <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.
[20] Global Privacy Enforcement Network <https://privacyenforcement.net/content/home-public>.
[21] OECD, Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD/LEGAL/0352.

international privacy enforcement authorities"[22]. Part of GPEN's Action Plan is to build a "network of networks"[23] comprising other privacy and data protection networks as well as other regulatory networks with interests that intersect with those of the GPEN's. One example is the 2024 Sweep in which GPEN teamed up with the International Consumer Protection Enforcement Network[24] to look at deceptive design patterns in websites and applications[25]. This is discussed in more detail in the next section as an example of the benefit of cooperation.

4. Applying the Pathetic Dot Model to International Data Protection Cooperation

When considering the Lessig Pathetic Dot Model in the context of international regulatory cooperation, it is easy to see the relevance of the law modality. All data protection and privacy regulators are creatures of law; created and given their powers and duties by legislation. Law sets out the requirements for organisations when processing personal data and the rights of individuals. Law provides the breach reporting and complaint mechanisms, frameworks for how regulators are required to handle such matters and the sanctions that can be issued for wrongdoing. As Lessig identified, law pushes regulated entities to behave as the State requires and will penalise those that do not comply.

As creatures of law in a digital world that knows no boundaries, it is perhaps inevitable that investigations into large data breaches is a focus for cooperation. Big breaches by big companies often require a big response, and one data protection authority may see benefits in joining forces with a like-minded regulator from another jurisdiction.

A recent example of international cooperation was the joint investigation into a breach by genetic testing company 23andMe, conducted by the Office of the Privacy Commissioner of Canada (the OPC)[26] and the UK's Information Commissioner[27] (the ICO). This collaboration is perhaps not surprising, given that both regulators were key contributors to the Enforcement Cooperation Handbook[28] that outlines how, amongst other activities, joint investigations can be conducted.

---

[22] Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.

[23] Global Privacy Enforcement Network 'Action Plan for the Global Privacy Enforcement Network (GPEN)' <https://privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen>.

[24] ICPEN <https://www.icpen.org/>.

[25] Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.

[26] Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.

[27] ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>.

[28] Global Privacy Assembly 'An Enforcement Cooperation Handbook' <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.

In October 2023, an individual claimed that they had breached 23andMe's systems and had copies of personal data that they were offering for sale. Later that month, the OPC and the ICO were advised by 23andMe that a number of affected individuals came from their jurisdictions.

Whilst the two jurisdictions had their own legislation, there were sufficient similarities to make a joint investigation viable, made possible by a Memorandum of Understanding between the two regulators, "pursuant to section 23.1 of PIPEDA[29] and Article 50 UK GDPR". The outcome of the joint investigation, issued in June 2025, was the finding of breaches under both PIPEDA and the UK GDP that during the investigation 23andMe had addressed such that the issues were deemed resolved[30]. However, in an example of a difference between legislative frameworks, the ICO had the power to fine and issued a monetary penalty of £2,310,000[31] on top of the finding.

Leveraging the law modality of the Pathetic Dot Model seems natural for data protection and privacy regulators and cooperation with international counterparts can expand a regulator's capacity and amplify their impact. However, investigations can be lengthy and resource intensive and are focused only on the behaviour of one organisation. There can be no doubt of the effectiveness of an investigation and sanction on 23andMe. During the investigation, whilst under the microscope of two regulators, the company addressed its shortcomings and improved its compliance. But it can be difficult to judge the impact of that case on other organisations, whether the lessons learnt by 23andMe are acted on by other organisations and whether the fine issued acts as a deterrent. It is with this in mind that the other three modalities of the Pathetic Dot Model should be considered and how, through international cooperation, these can be leveraged by data protection and privacy authorities to regulate behaviour.

To demonstrate this, this paper will discuss two examples of international cooperation used by the Office of the Data Protection Authority of Guernsey[32] (the ODPA). As one of the smallest data protection authorities in the world[33], it has looked to international cooperation to both provide additional capacity for action and to increase the impact of its actions. As an international finance centre, the Bailiwick of Guernsey[34] (the Bailiwick) is already punching above its weight, and a robust data protection regime can help secure that position. Further, as technology does not respect geographical boundaries, the Bailiwick's citizens face the same data protection

[29] Personal Information Protection and Electronic Documents Act (PIPEDA).
[30] Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.
[31] ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>.
[32] formally known in the Data Protection (Bailiwick of Guernsey) Law, 2017 as the Data Protection Authority
[33] 14 staff at time of writing.
[34] The Bailiwick of Guernsey comprises the islands of Guernsey, Alderney, Sark and Herm and is located in the English Channel. As a British Crown Dependency, it is a self-governing jurisdiction, with allegiance to the British Crown.

and privacy problems as much larger jurisdictions and deserve a regulator that can represent them on the international stage whilst adding value and benefits locally.

In 2024, the ODPA became a signatory to the joint statement on data scraping and the protection of privacy[35], an initiative of the GPA's IEWG. This joint statement, endorsed by 14 international data protection authorities, outlined the privacy risks from data scraping, how social media companies and operators of other websites could protect users' data, and the actions individuals could take to protect themselves. As the Bailiwick's Commissioner, Brent Homan, said, "Data-scraping poses a global risk that calls for a global response [...] In joining forces with our international data protection partners we are setting out key global expectations for social media companies towards ensuring adequate safeguards to combat non-authorised scraping"[36].

Following the issuance of the joint statement in August 2023, the signatories engaged with the leading social media companies to understand the technical challenges they faced in combatting unlawful data scraping and the actions they were taking. The virtual meetings allowed the ODPA to question these companies directly, something that would have been almost impossible without the combined weight of the other regulators involved in this initiative. Signatories also met with representatives of the Mitigating Unauthorized Scraping Alliance[37] (MUSA), a body that brings together "industry leaders to protect data from unauthorized scraping and misuse"[38].

The information gleaned in these important meetings led to the publication of a concluding joint statement that outlined additional expectations including that the training of AI large language models should be cognisant of data protection and privacy legislation, that safeguarding measures deployed to combat unlawful scraping should be reviewed regularly to keep pace with advancing technology and that data scraping permissible for commercial or societally beneficial purposes must be done lawfully[39].

Considering this initiative in terms of the Pathetic Dot Model, the law modality is at play as the basis for the expectations laid out in the joint statements were the legal obligations placed on organisations when processing personal data. However, this was not the only modality in play. By engaging with leading social media companies, the signatories were asking the market to apply its own pressure on entities to behave in an acceptable manner.

Whether it be by using their own compliant practices as a competitive advantage, appealing to privacy-conscious individuals or by calling out bad practice, getting the market or industry to act as a gatekeeper can be the extra push outliers need. This leveraging of the market was further demonstrated by the engagement with MUSA.

[35] ODPA 'ODPA joins international efforts to prevent unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=5a294e41-9eea-ee11-a204-6045bd8c5a56>.
[36] Ibid.
[37] MUSA <https://antiscrapingalliance.org/>.
[38] Ibid.
[39] ODPA 'Guernsey joins global partners to combat unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=f5ed30b6-3595-ef11-8a69-6045bdf2d3b5>.

This body was already in existence and seeking to promote good practice whilst raising public awareness. It was of benefit to MUSA to be seen to be engaging with regulators but, in turn, it was another opportunity for regulators to move the market modality, to the benefit of individuals and compliant companies alike.

In addition to making use of the market modality, through press releases and speaking engagements, the ODPA was able to leverage the societal norms modality. It provided opportunities to educate the public as to how their personal data could be used in a way they were neither expecting nor happy with. This empowers them to take steps to protect themselves, either by limiting the data they share with web-based platforms or by making choices based on how responsible the operator may be. By challenging the idea that 'that's the way it's always been and there is nothing I can do about it', external communications may activate the public to alter the societal norm and thus exert pressure on regulated entities.

Anecdotal evidence suggests that following ODPA press releases, data scraping became a topic of conversation between individuals and across boardroom tables showing that engaging with other modalities can spread a message and influence a narrative.

A further example of the power of international cooperation was the 2024 GPEN Sweep[40]. The topic was deceptive design practices or 'dark patterns', those aspects of website and app design that pushes the least privacy-friendly option to the benefit of the company and detriment of the individual. The Sweep saw GPEN join forces with the International Consumer Protection Enforcement Network[41], its consumer protection counterpart, to review websites and apps for indicators of dark patterns.

Over a thousand websites and apps were 'swept' as part of this initiative, by 26 privacy enforcement authorities and 27 ICPEN authorities making the Sweep "the most extensive example of cross-regulatory cooperation between privacy and consumer protection authorities, to date"[42]. Overall, 97% of websites and apps reviewed showed at least one indicator of deceptive design patterns[43].

One prominent industry in the Bailiwick of Guernsey is egambling. This sector is subject to regulation by the Alderney Gambling Control Commission[44] (the AGCC). Given the prevalence of problem gambling and the vulnerability of some users of egambling websites and apps, the ODPA focused its Sweep on those companies licensed by, and provided its results to, the AGCC. At the beginning of February 2024, 19 companies were 'swept' and each was found to have at least one indicator of

[40] Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>
[41] ICPEN <https://www.icpen.org/>.
[42] Global Privacy Enforcement Network 'GPEN Sweep 2024: "Deceptive Design Patterns" Report' <https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf>.
[43] Ibid.
[44] Alderney Gambling Control Commission <https://www.gamblingcontrol.org/>.

deceptive design practices with particular concerns about the transparency of processing[45].

As a result of the Sweep, the ODPA wrote to each company swept outlining its concerns both across the industry as a whole and specifically in relation to their own websites and apps. In less than three months, the ODPA received commitments from 78% of those companies to improve their practices and specifically address the concerns[46]. In one case, the data protection officer welcomed the ODPA's correspondence as it restated concerns they had expressed previously internally and the ODPA's intervention helped them secure the change they were seeking.

In an example of the market and societal norms modalities in action, by the end of 2024, all companies had committed to improvements. The last company confirmed its commitment following an industry conference at which the ODPA's Commissioner expressed his appreciation to those companies that had committed to change. It realised that it was vulnerable to being cast in a poor light by its industry counterparts (market modality) and that users were expecting better (societal norms modality). Whether it was a case of self-interest or a genuine desire to improve, the ultimate outcome was a remarkable 100% commitment to improve, an action that would have taken many years if tackled through investigations.

Turning to the fourth modality – architecture - with technology moving apace and providing its own behavioural constraints whilst embracing innovation the clearer regulators are about their expectations and the more consistent those expectations are across the globe, the more developers can build these expectations into their products. In the run up to the GDPR coming into force, organisations' inboxes were flooded with adverts for technical solutions for GDPR. Some were more legitimate than others but it shows that an emphasis on accountability and privacy by design drove technological developments.

Activities such as the GPEN Sweep or the joint data scraping statements set out expectations and requirements. The enthusiasm of developers to provide solutions for common problems that they can market as responding to regulators expectations can see the architecture modality applying its own pressure to the pathetic dot. Cooperation by regulators can see global technical solutions to global technical problems.

[45] ODPA 'ODPA examines Bailiwick's gambling sector for harmful privacy practices as part of global sweep' <https://www.odpa.gg/news/news-article/?id=baea8752-d03d-ef11-8409-7c1e5226329b>.

[46] ODPA 'Bailiwick's gambling sector pledges to make improvements after ODPA shares concerns of harmful privacy practices' <https://www.odpa.gg/news/news-article/?id=cd258672-9f79-ef11-a670-6045bd97f872>.

5. Conclusion

Lawrence Lessig's 'Pathetic Dot Model' shows that whilst data protection and privacy are legal constructs, the reality is that there is more than just the law that acts to regulate the behaviour of the entity, or dot, that is being regulated. Pressure, constraints and impetus can be applied as effectively through the societal norm, the market and the architecture with which the entity interacts and the four modalities can be harnessed to drive improvements to the benefit of all stakeholders.

Importantly, whilst this can be achieved by data protection and privacy regulators acting on their own, international cooperation can strengthen these modalities and seek to resolve the problems posed by differing legislative mechanisms. This paper also shows that international cooperation does not have to be in the form of resourcing intensive joint investigations to lead to a positive change. A clear, consistent position adopted by regulators from across the globe can have as much, if not more, impact on the entity as a hefty fine issued to a competitor.

International cooperation is an invaluable tool in a regulator's arsenal. Whether a large or small regulator, one with many years in the game or one just starting out, international cooperation can expand capacity and amplify impact.

Bibliography:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119.
2. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 (opened for signature 28 January 1981).
3. Paris Agreement to the United Nations Framework Convention on Climate Change, adopted December 12, 2015, T.I.A.S. No. 16-1104.
4. Climate Change Act 2008 (c. 27).
5. *OECD,* Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD/LEGAL/0352.
6. *Lessig L,* Code and the Other Laws of Cyberspace (Basic Books 1999).
7. *Lessig L,* Code Version 2.0 (Basic Books 2006).
8. Alderney Gambling Control Commission <https://www.gamblingcontrol.org/>.
9. BBC News 'GDPR: Are you ready for the EU's huge data privacy shake-up?' <https://www.bbc.co.uk/news/technology-43657546n>.
10. Council of Europe 'Chart of signatures and ratifications of Treaty 108' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.

11. Global Privacy Assembly <https://globalprivacyassembly.org/>.
12. Global Privacy Assembly 'An Enforcement Cooperation Handbook' <https://globalprivacyassembly.org/wp-content/uploads/2021/11/enforcement-cooperation-handbook-en-202111.pdf>.
13. Global Privacy Assembly 'History of the Assembly' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/>.
14. Global Privacy Assembly 'International Enforcement Cooperation Working Group Report – July 2024' <https://globalprivacyassembly.org/wp-content/uploads/2024/11/9.-IEWG-GPA-Annual-Report-2024.pdf>.
15. Global Privacy Assembly 'Mission and Vision' <https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision/>.
16. Global Privacy Assembly 'Strategic Plan 2023 – 2025' <https://globalprivacyassembly.org/wp-content/uploads/2024/02/GPA-Strategic-Plan-final-version-update-oct10-1.pdf>.
17. Global Privacy Assembly 'Working Group Reports' <https://globalprivacyassembly.org/document-archive/working-group-reports/>.
18. Global Privacy Enforcement Network <https://privacyenforcement.net/content/home-public>.
19. Global Privacy Enforcement Network '2024 GPEN Sweep on deceptive design patterns' <https://privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns>.
20. Global Privacy Enforcement Network 'Action Plan for the Global Privacy Enforcement Network (GPEN)' <https://privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen>.
21. Global Privacy Enforcement Network 'GPEN Sweep 2024: "Deceptive Design Patterns" Report' <https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf>.
22. ICO '23andMe' <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>
23. ICPEN <https://www.icpen.org/>.
24. MUSA <https://antiscrapingalliance.org/>.
25. ODPA 'Bailiwick's gambling sector pledges to make improvements after ODPA shares concerns of harmful privacy practices' <https://www.odpa.gg/news/news-article/?id=cd258672-9f79-ef11-a670-6045bd97f872>.

26. ODPA 'Blog: Dark patterns and the gambling industry' <https://www.odpa.gg/news/news-article/?id=dccb80cb-3156-ef11-bfe3-000d3a2d37f7>.
27. ODPA 'Guernsey joins global partners to combat unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=f5ed30b6-3595-ef11-8a69-6045bdf2d3b5>.
28. ODPA 'ODPA examines Bailiwick's gambling sector for harmful privacy practices as part of global sweep' <https://www.odpa.gg/news/news-article/?id=baea8752-d03d-ef11-8409-7c1e5226329b>.
29. ODPA 'ODPA joins international efforts to prevent unlawful data scraping' <https://www.odpa.gg/news/news-article/?id=5a294e41-9eea-ee11-a204-6045bd8c5a56>
30. Office of the Privacy Commissioner of Canada, 'Concluding joint statement on data scraping and the protection of privacy' <https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2024/js-dc_20241028/>.
31. Office of the Privacy Commissioner of Canada 'Joint investigation into a data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner' <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/>.
32. Office of the Privacy Commissioner of Canada, 'Joint statement on data scraping and the protection of privacy' <https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/js-dc_20230824/>.
33. UN Trade & Development, 'Data Protection and Privacy Legislation Worldwide' <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

Giovanni Maria Riccio[*]

Brussels Effect, Data Protection and AI Act

This article explores the role of comparative law in understanding and addressing the legal challenges posed by emerging technologies. It addresses the following issues: the reasons why the European Union sets global regulatory standards, illustrated by the example of the GDPR; the factors behind the United States' capacity for innovation; and the potential future circulation of the EU legal model.

Keywords: *Data Protection, European Union, GDPR, regulatory law, private law, AI Act, Brussels Effect, legal fragmentation, neoliberalism, digital markets, Chinese tech companies, compliance challenges.*

1. The Usefulness of Comparative Law in the Study of Emerging Technologies

Addressing the topic of artificial intelligence from a comparative legal perspective is no easy task. It requires, as a preliminary step and in order not to create unrealistic expectations for readers, a clarification of the analytical scope. Those seeking detailed information on the specific regulations of various legal systems should be advised to stop reading and turn to more profitable activities.

Indeed, it should be common knowledge—though it bears repeating—that comparative law is essentially a method, even if the scholarly debate on the methods and functions of comparative legal studies appears to be losing momentum[1]. However, we can certainly say what comparative law is *not*: it is *not* the study of foreign legal systems per se, nor is it merely a compilation of legal information—it is, above all, comparison[2].

---

[*]Founder and Senior Partner at e-Lex Law Firm (Rome); Full Professor of Comparative Law; Current courses: Copyright Law, Cultural Heritage Law, Art Law - Università di Salerno/DPO.

[1] For an introduction to this aspect, see *Stanzione P.*, Sui metodi del diritto comparato, Introduzione a *Ancel M.,* Utilità e metodi del diritto comparato, trad. it., Camerino, 1974, XXIII, also in French on in Rev. *int. droit comparé*, 1973, 885; L.-J. Costantinesco, Il metodo comparativo, ed. it., Torino, 2000.

[2] According to *Sacco R.*, Circolazione e mutazione dei modelli giuridici, in Dig disc. priv., sez. civ., II, Torino, 1988, 365, If comparative law were merely the analysis of foreign legal systems, its function would be limited to a descriptive exercise, lacking any real impact on the understanding and development of domestic law. Instead, comparative law offers a method for critically examining one's own legal system, revealing not only its distinctive

Comparative law does, of course, serve to explore alternative solutions, but it is also a valuable tool for deepening our understanding of domestic law. It does not confine itself to the analysis of legislative texts but aspires to move beyond legal formalism. It begins with the study recent decades, even identifying these formants—or rather, outlining their boundaries—has become increasingly complex. Consider, for example, the legislative formant national law, supranational law, and the decisions and measures issued by independent administrative authorities all now coexist and interact.

For decades now, we have been witnessing the rise of polycentric law, resulting from the erosion of the state's monopoly over the production of legal norms[3]. This is a product of economic globalization, where national legislative sovereignty must now coexist with new centers of legal norm production, including international economic and professional communities[4]. Sometimes this law is not imposed from above but emerges spontaneously from international commercial practices; other times, it is state law enriched with prescriptive content from private rules—as is the case with references to harmonized standards in the AI Act[5].

It is enough to observe that most legal norms governing innovation today originate from the European Union, including those related to artificial intelligence. At the Union level, there has been a marked shift away from directives in favor of regulations, signaling a transition from legal harmonization to uniformization. This choice reflects, among other factors, the desire of some national legal systems to preserve their own legislative sovereignty—often in response to political or lobbying pressures—which, however, risks undermining the EU's stated objective in this field: the creation of a barrier-free internal market that realizes the core aims of the Treaties.

features but also its potential shortcomings or inefficiencies in comparison with alternative legal models. (Still *Sacco R.*, Introduzione al diritto comparato, in Tratt. dir. comp. dir., da R. Sacco, 5ª ed., Torino, 1992).

[3] Cf. *Ferrajoli L.*, Crisi del diritto e dei diritti nell'età della globalizzazione, in Questione Giustizia, 2023, <https://www.questionegiustizia.it/articolo/crisi-del-diritto-e-dei-diritti-nell-eta-della-globalizzazione>.

[4] Here too, the bibliography could be vast; however, for a methodological analysis as well, reference is made to *Grossi P.*, Aspetti giuridici della globalizzazione economica, in I Georgofili. Atti della Accademia dei Georgofili» 2013.

[5] The harmonized standard, according to Regulation (EU) No 1025/2012, is a technical specification adopted by a European standardization body (for example, CEN – the European Committee for Standardization; CENELEC – the European Committee for Electrotechnical Standardization; ETSI – the European Telecommunications Standards Institute) based on a request made by the European Commission. These standards are developed to facilitate the implementation of European Union legislation and to ensure a more efficient single market. The process of creating a harmonized standard involves several steps. First, the European Commission issues a mandate identifying a regulatory need and entrusts one of the European standardization bodies (CEN, CENELEC, or ETSI) with the task of drafting a specific standard. These bodies then develop the standard, involving technical experts and stakeholders in the drafting process to ensure the standard meets market needs and complies with EU legislation. Finally, the standard is adopted and published in the Official Journal of the European Union. However, Recital 117 introduces an additional requirement, stating that the harmonized standard must be "considered suitable for governing the relevant obligations by the AI Office." Therefore, it must be understood that, in addition to the Commission's mandate, a subsequent "endorsement" by the AI Office is required in order for the harmonized standard to benefit from the presumption of conformity.

Moreover—and again this is common knowledge among comparatists—the analysis of legal formants must necessarily be coupled with that of crypotypes[6]: the constellation of elements—linked to a people's legal tradition, modes of knowledge transmission, social and cultural context, and economic environment—that shape the training and worldview of legal professionals. This becomes particularly important when moving beyond the Western Legal Tradition. As the legal regulation of AI technologies inevitably requires, we often encounter non-Western legal systems whose lawyers and policymakers are shaped by a distinct hierarchy of values—one that may differ significantly from that of their Western counterparts.

Nor can we overlook, especially in the context of regulating AI systems, the increasingly central role played by ethics, which ought to guide the design of such systems in order to avoid discriminatory biases or exploitations contrary to the shared values of the international community. On this point, it is important to note that the semantic scope of the term "etica" (ethics) in romance languages does not entirely overlap with the broader Anglo-American concept of "ethics": in the former, ethics has primarily a subjective connotation, separate from legal norms, which follow formal criteria for their selection; in the latter, ethics is more expansive, often embedded in forms of soft law, such as codes of ethics or conduct.

To define comparative law as a method is to recognize that it goes beyond mere data collection on foreign legal systems[7]. This legal field does not simply involve listing and analyzing rules from different countries, but rather focuses on identifying the structures, principles, and solutions adopted within various legal contexts. In this paper, we aim to outline some of the main features that characterize the European and U.S. systems. For reasons of brevity, we will deliberately set aside the insights that might emerge from an analysis of Asian legal systems. We will not focus on individual legal institutions but instead seek to identify prevailing elements that underlie legal policy choices.

This approach stems from an awareness of the profound transformation of legal systems over the last thirty years. In an era of growing interconnection among states, comparative law plays an increasingly crucial role, as legal systems no longer exist in isolation but continuously interact through international treaties, supranational institutions, and processes of legal reception and harmonization[8].

[6] Cryptotypes, in comparative law, are those implicit elements of a legal system that do not find direct expression in the formal sources of law (legislation, case law, and doctrine) but deeply influence the functioning and application of norms. They include cultural values, established practices, legal mindsets, and unwritten principles that determine how law is interpreted and applied in a given society. The concept of cryptotypes was developed by Rodolfo Sacco, who highlighted how, alongside explicit formants, there exist these latent elements that shape the law of a legal order. They are particularly relevant when analyzing legal systems belonging to different traditions, as they allow for an understanding of the real legal dynamics beyond the normative data.

[7] *Gorla G.*, Diritto comparato, in Enc. dir., XII, Milano, 1964, 930; *Ascarelli T.*, Premesse allo studio del diritto comparato, in Studi di diritto comparato e in tema di interpretazione, Milano, 1952, 6 ss.

[8] *Mattei U.*, Comparative Law and Economics, Univ. of Michigan Press, 1997; *Hoecke Van M.*, Epistemology and Methodology of Comparative Law, Hart Publishing, 2004; *Zeno-Zencovich V.,* Comparison Involves Pluralism*:* A Rejected View-Point, in Comparative Law Rev., 2025, 6.

Finally, the comparative approach requires a rejection of formalism and a move beyond the mere analysis of legislation. It calls for consideration of the many factors influencing the creation and application of law, including extra-legal reasons, the interplay among different legal formants, and their mutual influence. For this reason, as anticipated, we will focus on comparing the political (and thus legal) rationales behind the different regulatory approaches adopted in the field of artificial intelligence.

2. Why the European Union Makes the Rules: The Example of the GDPR

A pervasive narrative has taken hold in mass media rhetoric—one that is highly reductive and lacks empirical support—claiming that the United States innovates, China copies, and the European Union regulates. Beyond the oversimplification, this assertion deserves closer examination to understand the reasoning behind such a classification.

Let us begin at the end—that is, with the idea that Europe invests little in innovation but excels in producing legal norms.

This assumption is misleading when viewed in percentage terms, but unfortunately realistic in absolute terms. A recent edition of the EU Industrial R&D Investment Scoreboard, published in December 2024, reported that in 2023, European industry outpaced the growth of U.S. (+5.9%) and Chinese (+9.6%) companies for the first time, with a growth rate of 9.8%.

While encouraging, this figure does not account for three important factors.

First, the wide disparities among EU Member States, with higher peaks in more advanced countries like France and Germany, while others—including Italy—lag behind; second, that these percentages refer to vastly different absolute values; and third, that European investments are often spread across many small-scale projects rather than concentrated in a few strategic initiatives. The Horizon 2020 programme is a case in point: it funded numerous small entrepreneurial ventures, not all of which yielded industrial outcomes.

Then there is the matter of regulation, grounded in the concept—now widely known and perhaps declining—of the so-called Brussels Effect. This refers to the EU's ability to project its regulatory influence beyond its geographic and jurisdictional borders, shaping business practices, national legal frameworks, and even international agreements.

A central pillar of the Brussels Effect[9] is the extraterritorial application of EU law: regulations apply not only to entities based within the Union, but also to those outside

[9] The term is due to *Bradford A.*, The Brussels Effect: How the European Union Rules the World, Oxford Univ. Press, 2020. The author identifies the key to this regulatory influence in the size of the European internal market, combined with strong regulatory capacity: to access the EU market, global companies comply with European standards, ultimately applying them also in other markets, producing a de facto harmonization effect. The book

it that offer goods or services within the EU market or process data of EU citizens. The most paradigmatic example is the General Data Protection Regulation (GDPR), which applies to data controllers outside the EU whenever they process personal data of individuals located within the Union (Art. 3 GDPR). This creates a need for many non-EU companies to adapt their data practices to EU standards. This normative reach is justified both by the effects doctrine under international law and by the EU's market power, whereby access to the internal market requires compliance with its rules[10].

Beyond formal extraterritoriality, global companies frequently adopt EU standards voluntarily—or more precisely, *de facto*—for reasons of regulatory consistency and economic efficiency. It is often simpler to adhere to a single, stringent standard—typically the EU one—rather than customize compliance for each market. This is especially true in areas like environmental protection, food safety, privacy, and competition law.

Once again, the GDPR provides a clear example: tech giants like Google, Apple, and Microsoft have adopted GDPR-inspired data protection policies globally, even in contexts where they are not formally required to do so. Similarly, in the environmental field, Japanese and U.S. automakers have aligned their emission standards with EU requirements to maintain market access, often extending those standards globally[11].

Another vector of the Brussels Effect is regulatory imitation by third countries that lack the economic clout of the United States. The technical quality, internal coherence, and market-driving effect of EU rules have made them a model for many national legislations. Imitation may stem from pragmatic goals (e.g. facilitating EU market access) but also from legal prestige and a desire for normative convergence.

---

shows how this occurs in strategic sectors such as personal data protection (GDPR), food safety, competition, environmental sustainability, and finance, building a narrative according to which the Union acts as a "regulatory superpower," capable of setting the global rules of the game despite lacking an explicit imperial or coercive strategy. The analysis is distinguished by its legal-economic approach, but also by a political reading that recognizes European regulatory power as a form of institutional soft power, founded on technocracy, procedural transparency, and the attractiveness of the European regulatory model. The Brussels Effect thus emerges as a predominantly unilateral process, not the result of multilateral negotiations, but rather of the EU's structural power and the economic rationality of global companies.

[10] *Bradford A., note* 9, 5: "the EU can unilaterally externalize its laws outside its borders through market mechanisms".

[11] The Brussels Effect also extends to the international level, both through the spread of European standards in multilateral trade agreements and through their adoption in technical standards by supranational organizations such as ISO (International Organization for Standardization), the Codex Alimentarius Commission, or ICAO (International Civil Aviation Organization). In the context of trade agreements, the EU has often included regulatory clauses that require the adoption of European standards or equivalent ones. This is the case with Association Agreements or free trade agreements (e.g., CETA with Canada, EPA with Japan), which include provisions on environmental sustainability, data protection, and product safety. In such agreements, the EU imposes minimum requirements, helping to extend its standards to third countries. Beyond the legal framework, it is important to highlight how the Brussels Effect also manifests informally and technically through the definition of harmonized rules and industrial norms. Many European technical standards become global practice due to their rigor and practical usefulness. Multinational companies adopt them to avoid the risk of having to design differentiated products for different markets. The spread of technical standards can be further facilitated by soft law—that is, non-binding instruments (guidelines, recommendations, codes of conduct) produced by European agencies or standardization bodies. The example of the codes of conduct provided for by the GDPR (Articles 40–41), although not mandatory, shows how these tools can act as catalysts for regulatory convergence, especially in technological or digital sectors.

The most fertile ground for this effect has been data protection law. But in environmental law too, the EU's regulation of chemicals (REACH) has served as a model for countries like China and Turkey, fueling a phenomenon of unilateral regulatory globalization—not through imposition, but through voluntary alignment with EU standards, for reasons of compatibility and strategic advantage[12].

In the case of the GDPR, imitation has ranged from literal replication to selective adoption—most notably of the accountability principle under Art. 5(2), which requires the controller (the entity determining the purposes and means of processing) to ensure that fundamental data protection principles—lawfulness, fairness, transparency, data minimization, integrity, etc.—are upheld not through a fixed list of obligations, but by demonstrating that processing ensures adequate protection of data subjects' rights and freedoms.

For example, Brazil's Lei Geral de Proteção de Dados (LGPD)—Law No. 13.709 of 2018—bears strong resemblance to the GDPR[13]: it applies to all entities (public or private, natural or legal) that process personal data of individuals located in Brazil, regardless of the data controller's location; it requires clear and comprehensive disclosure to data subjects; mandates impact assessments for high-risk processing; and obliges maintenance of a processing activity register[14].

Article 50 of the LGPD allows controllers and processors—individually or via associations—to develop codes of good practice and governance, internal oversight mechanisms, risk mitigation strategies, and especially technical and security standards. On this point, the LGPD and GDPR diverge: while the latter allows for the drafting of codes of conduct, it does not clearly regulate the definition of common technical and security standards, leaving operators with some uncertainty regarding best practices.

Brazilian law further provides that data governance policies should be based on a systematic risk-impact assessment, proportionate to the organization's size, scope of activities, and data sensitivity. Like the GDPR, Article 50 of the LGPD requires controllers to demonstrate the adequacy of adopted measures; however, the inclusion of a minimum baseline of mandatory safeguards arguably makes compliance easier—at least procedurally—for Brazilian companies and administrations.

A similar comparative analysis applies to Switzerland's revised data protection law, which came into force in 2020 after a legislative process that began in 2017. Among other elements, legal persons are no longer included in the definition of "personal data"; as in Brazil, controllers must keep a processing register; impact

[12] See *Almada M., Petit N.,* The EU AI Act: A Medley of Product Safety and Fundamental Rights, EUI, RSC, Working Paper, 2023/59.

[13] *Liz dos Santos A.L.*, Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais", Revista dos Tribunais, (2020), 105.

[14] For further details, see *Viola M., L. Heringer.,* Um olhar internacional: Lei Geral de Proteção de Dados Pessoais (LGPD) e o General Data Protection Regulation (GDPR), adequação e transparência internacional de dados, in *Souza C.A., Magrani E., Silva P., (eds.),* Lei Geral de Proteção de Dados(LGPD): caderno especial, São Paulo, Thomson Reuter, 2019, 227.

assessments are required for high-risk processing; and personal data breaches must be reported to the supervisory authority (the Federal Data Protection and Information Commissioner)[15].

Swiss law also mandates the appointment of a local representative for controllers based abroad. Regarding data subject rights, the new law introduces, in line with the GDPR, the right to data portability and the right not to be subject to solely automated decisions. It also incorporates privacy by design and by default, as well as data minimization principles. The supervisory authority's powers have been expanded to include inspections and binding decisions.

Many other countries have adopted GDPR-inspired regulations, including Nigeria's Data Protection Regulation (NDPR), issued in January 2019, and Egypt's Law No. 151 of 2020. For smaller nations, this reflects a clear desire to facilitate trade with the EU, beyond the legal prestige the GDPR has clearly achieved. Switzerland's alignment seems almost inevitable, given its geographic location, though it remains outside the EU. What is more surprising is that a global economic power like Brazil has adopted such similar standards.

A separate—albeit brief—treatment is warranted for China's data protection reform. The Personal Information Protection Law (PIPL) came into force on November 1, 2021, after a lengthy legislative debate. It likely represents a major shift in the global legal landscape, as China has adopted several EU-inspired regulatory elements, replicating many GDPR provisions[16].

The law's scope covers three primary scenarios:

a) Processing activities carried out within China;
b) Provision of goods or services to Chinese citizens, or analysis of their behavior;
c) Other cases specified in national laws.

When a foreign entity processes personal data under PIPL's jurisdiction, Article 53 requires it to establish a presence in China or appoint a representative, whose details must be submitted to the authorities. Article 72 echoes the GDPR by exempting personal or domestic data processing from PIPL's scope.

The PIPL mirrors the GDPR in distinguishing between data controllers and processors, assigning them similar roles: controllers determine the purposes and means of processing; processors act under their direction. Strong parallels also emerge regarding the required information at the point of data collection, closely resembling Article 13 of the GDPR[17].

Sensitive data under PIPL includes religious beliefs and health data (as in the GDPR), but also financial information and personal assets—categories not classified as sensitive under EU law. Biometric data, information about minors under 14, and

[15] Cf. *Meier P., Métille S.,* Loi fédérale sur la protection des données, Helbing Lichtenhahn Verlag, 2023.

[16] *Moriconi C.*, Recent Evolution of the Personal Privacy Legal Protection in People's Republic of China, 9 Nordic Journal of Law and Social Research, (2019) 248; *Santoni G.*, Personal data as a market commodity: legal irritants from China "experience", 1 European Journal of Privacy Law and Technology, (2023), 1.

[17] *Creemers R.*, China's Emerging Data Protection Framework, (November 16, 2021), SSRN: https://ssrn.com/abstract=3964684.

geolocation data are all expressly included among sensitive categories—highlighting heightened global concern.

The legal bases for data processing under PIPL strongly resemble those in the GDPR. Consent must be freely given, specific, and revocable (Article 14). Like the GDPR, consent is not required if data processing is necessary for contractual obligations or legal compliance. Public health emergencies and life-or-death scenarios are also recognized as valid legal bases[18].

PIPL places significant emphasis on data transfers, requiring prior assessment procedures akin to the GDPR's DPIA—but with stricter conditions[19]. These assessments must evaluate the validity, necessity, and proportionality of the transfer; data categories and sensitivity; and the recipient's technical and organizational safeguards[20].

Article 40 requires these assessments to be carried out by the State Department for Cyberspace Administration and based primarily on security criteria. The obligation applies to critical infrastructure operators and controllers processing personal data above thresholds set by the same Department.

The major difference between the EU and Chinese models lies in the authority responsible for evaluation. In China, self-assessment is not permitted: public authorities must validate all measures, following uniform standards. In contrast, the GDPR gives controllers the freedom to adopt what they deem appropriate safeguards. In this sense, China's model appears more predictable—*formally*—but it also entails constant state surveillance of information flows.

The GDPR-PIPL parallel breaks down when shifting from private to public law, particularly in the relationship between state and citizens. The PIPL seems to move along two tracks: on the one hand, aligning with EU rules to facilitate commercial exchanges; on the other, preserving a clear distance in terms of public law approach[21].

[18] *Calzada I.*, Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL), 5 Smart Cities, (2022) 1140.

[19] Article 38 of the PIPL (Personal Information Protection Law) provides four distinct and alternative criteria for the transfer of personal data abroad: a) Passing a security assessment organized by the national Cyberspace Administration of China, in accordance with Article 40 of this law; b) Obtaining a personal information protection certification issued by a specialized body according to the provisions of the national Cyberspace Administration of China; c) Entering into a contract with the foreign recipient based on a standard contract formulated by the same Administration, which establishes the rights and obligations of both parties; d) Other conditions stipulated by laws or administrative regulations, or by the national Cyberspace Administration of China. The translation of the PIPL was made by Rogier Creemers and Graham Webster, based on the preliminary English version of the second draft revision of the law developed by DigiChina, and is available at the following link: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ For further discussion on the assessment to be conducted, see also *Zheng G.,* Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China, 43 Computer Law Security Rev. 105610, 2021.

[20] *Voss W. G., Pernot-Leplay E.,* China Data Flows and Power in the Era of Chinese Big Tech, 44 Nw. J. Int'l L. & Bus. (2024) 1.

[21] Cfr. *Pernot-Leplay E.,* China's Approach on Data Privacy fLaw: A Third Way between the US and the EU? 49 Penn State Journal of Law & International Affairs, (2020) 49, secondo cui la Cina rappresenterebbe un modello terzo rispetto a Stati Uniti ed Europa.

For instance, the definition of "sensitive data" includes any information whose unlawful disclosure might harm dignity, national security, or personal property—reflecting a stark imbalance between individuals and state authority. A special category—absent from EU law—covers data processing for journalistic, political, or public interest purposes.

Lastly, it is worth noting that PIPL does not hold a central position in China's digital regulatory framework as GDPR does in the EU. Rather, it is embedded within a broader legal architecture dominated by cybersecurity law. In a system where fundamental rights are subordinate to other state priorities, personal data protection remains a secondary concern.

3. Why the United States Innovates (or Would Innovate)

Let us now return to the initial assumption that the United States plays the role of the "great innovator" by analyzing the legislative approach that has supported technological development. While it is undeniable that the level of technological advancement among U.S. companies is unmatched by other countries, it is equally clear that political and legislative choices have significantly influenced this development.

The neoliberal rhetoric underpinning these choices has always relied on a core assumption: "technology changes exponentially, but social, economic, and legal systems change incrementally."[22] This introduces a problem of "pace," meaning that law evolves more slowly than technological progress, and thus institutions should refrain from imposing constraints on digital innovation until technologies have fully matured. However, this simplification deserves scrutiny. While it is true that technology moves faster than legislative processes, it is also true that the function of the law should be not only to drive technology forward but also to impose limits when technological developments endanger recognized and codified values.

The most insightful scholarship has referred to a "twentieth-century synthesis"—a neoliberal paradigm based on three key pillars: market efficiency as the supreme criterion, which overlooks issues of power and inequality; formal neutrality of legal

[22] These are the words of *Downes L.,* The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age, Basic Books, 2009. The book analyzes the impact of digital technologies on law and society, starting from the thesis that law and regulatory institutions evolve at a linear pace, while technology advances exponentially. This imbalance generates a regulatory disruption, where traditional legal rules struggle to adapt to new digital scenarios, giving rise to the nine "laws of disruption." These laws highlight how technology upends established sectors, rendering obsolete legal norms that were created in pre-digital eras. Issues such as privacy, intellectual property, platform liability, and data governance are addressed proactively, with a call to develop a more flexible, principle-based regulation capable of evolving alongside innovation. It is worth noting that, beyond influencing U.S. regulatory solutions, the book has had a significant impact on academic and policy debates concerning the need for agile and adaptive regulation. In fact, although not directly cited in legislative texts, this theory has contributed to shaping the European Union's legislative choices toward risk-based and technologically neutral approaches, as reflected in the GDPR, the Digital Markets Act, and the AI Act.

rules, which conceals underlying power dynamics; and an "anti-political" approach that reduces the role of democratic politics in favor of technical decision-making[23].

Furthermore, the adoption of law & economics paradigms and their doctrines—which dominated North American debates for decades—has shaped the very pillars of neoliberalism. Neoliberalism should not be seen as a natural outcome of market logic, as is often claimed or assumed, but rather as an institutional force shaped by law. Here, legislative and judicial components do not play a neutral role; they actively contribute to structuring markets, strengthening private powers, and influencing democratic capacity[24].

It is no coincidence that, in the United States—where no federal data protection regulation exists—legal scholarship still tends to define privacy as the "right to be let alone," rather than as control over the circulation and use of personal data. In other words, the U.S. remains far removed from the European paradigm of data protection as a fundamental right, and still clings to a proprietary notion of privacy—as a right to exclude others from one's private affairs or a proprietary control over one's own data. This approach fails to consider that the use of data, while aimed at protecting the individual, must give way to the collective interest when super-individual concerns arise[25].

In the field of artificial intelligence, a confused debate is currently underway between those advocating for a complete moratorium on any new regulation (even suggesting that existing laws be suspended for the next decade), and others—more cautiously—insisting on the need to establish safeguards and protections for citizens in the face of emerging technologies. The risk is a new phase of laissez-faire, allowing American companies to consolidate (or rather, strengthen) their oligopolistic positions in the market, unburdened by transaction costs or regulatory hurdles. This scenario recalls the late 1990s and early 2000s—the first "season" of the internet.

Analyzing the U.S. legal model is complicated by its federal nature and the resulting constellation of often-inconsistent state-level laws regulating technological innovation.

---

[23] See *Purdy J.S., Grewal D.S., Kapczynski A., Rahman S. K.*, Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis, 129 Yale L.J. 1784, 2020. This is, in our opinion, a seminal study, as it theorizes the so-called Law and Political Economy (LPE) approach. It challenges the dominant view that law should merely ensure neutral market conditions while allowing economic actors to operate freely without structural interference from the state—a view that proves inadequate for understanding contemporary dynamics of inequality, economic power, and democratic crisis. The authors argue that law is never neutral; rather, it plays a constitutive role in organizing the economy and distributing resources and power. The article calls for a rethinking of legal institutions as tools for social transformation, promoting economic justice, inclusion, and substantive democracy. It has significantly influenced academic debate, particularly in areas such as digital regulation, labor, environmental law, and racial equity.

[24] Cf. *Kennedy D.*, Law-and-Economics from the Perspective of Critical Legal Studies, in P. Newman (ed.), The New Palgrave Dictionary of Economics and the Law, London, 2002, <duncankennedy.net/wp-content/uploads/2024/01/law-and-economics-from-the-perspective-of-cls.pdf>.

[25] A paradigmatic example is the undoubtedly valuable and scientifically rigorous work by *Richards N.,* Why Privacy Matters, Oxford University Press, 2021.

However, two examples are paradigmatic.

In 1996, the *Communications Decency Act* (CDA) was enacted under the Clinton administration as a response to the growing issue of child pornography online[26]. Senator Exon, the Act's main proponent, intended to curb the proliferation of online pornography and, in particular, to restrict minors' access to such content[27]. The potential threat posed by the internet—as a sort of red-light district—prompted the creation of this Act, which was heavily criticized by scholars as a liberticidal measure against internet development (and ultimately challenged before the Supreme Court in *Reno v. ACLU*)[28].

One key provision was the *Good Samaritan Clause*—§ 230(c)(2)(A)—which granted immunity to internet service providers (ISPs) acting in good faith to restrict access to material deemed obscene, offensive, or otherwise harmful, even in the absence of specific constitutional protections. Over time, this clause not only influenced defamation law but also became a legal shield for ISPs to avoid removing user-posted content.

[26] Following the adoption of the Act under consideration, part of the legal scholarship proposed an alternative solution for the regulation of online pornography assigning websites a second-level domain (e.g., .sex or .osc) capable of indicating, *prima facie*, the obscene nature of the content. See *Major A. M., Internet Red Light District:* A Domain Name Proposal for Regulatory Zoning of Obscene Content, in *Marshall J.* Computer & Info. 21, 1997.

[27] "The information superhighway should not become a red-light district. This legislation will keep that from happening and extend the standards of decency, which have protected telephone users to new telecommunications devices. Once passed, our children and families will be better protected from those who would electronically cruise the digital world to engage children in inappropriate communications and introductions. The Decency Act will also clearly protect citizens from electronic stalking and protect the sanctuary of the home from uninvited indecencies", 141 Cong. Rec. S1953. See also "The fundamental purpose of the Communications Decency Act is to provide much needed protection for children," 141 Cong. Rec. S8088. The legislative proposal was inspired by a study by M.R. Imm, Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories, 83 Georgetown L.J. 1849 (1985), which claimed that 83.5% of content distributed online was pornographic in nature. The study, however, raised significant concerns among both U.S. legal scholars and system operators. For a summary of the criticisms, see *Cannon R*., The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway, 49 Fed. Comm. L.J. 52 (1996). On the subject of obscenity, the leading precedents include Miller v. California, 413 U.S. 15 (1973), which established the standards for evaluating obscenity (the so-called obscenity test), and Paris Adult Theatre I v. Slaton, 413 U.S. 49 (1973), which recognized the State's interest in regulating the commercial distribution of obscene and pornographic materials, as well as public performances of such nature. At the legislative level, obscenity is governed by Chapter 71 of Title 18 of the United States Code, while § 223 of Title 47 addresses "Obscene or Harassing Telephone Calls." It is worth recalling that obscenity is one of the rare forms of speech not protected by the First Amendment. Naturally, the possession and distribution of child pornography are also prohibited; see 18 U.S.C. § 2251; Osborne v. Ohio, 495 U.S. 103 (1990). Finally, in 1998, the Protection of Children from Sexual Predators Act was enacted to combat online child exploitation.

[28] 521 U.S. 844 (1997). The Supreme Court struck down only §§ 223 (a) and (d) of the law, which prohibited "the knowing transmission of obscene or indecent messages to any recipient under 18 years of age" and "the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age." It should also be noted that in 2001, the Children's Internet Protection Act and the Neighborhood Internet Protection Act came into force. These laws require library operators to install filtering software on their computers that provide internet access to users, in order to block the display of pornographic material.

In retrospect, § 230—despite its excesses—enabled the expansion of services offered by the then-new internet players, who benefited from a kind of immunity by not being required to remove third-party content.

A second significant example is the *Digital Millennium Copyright Act* (DMCA) of 1998, which introduced provisions to protect ISPs from copyright infringement claims, affirming the principle of technological neutrality—later mirrored in the EU E-Commerce Directive (2000/31/EC)[29].

The DMCA rules—subsequently adopted in the EU—exempted ISPs from liability for illegal content uploaded by users, provided such content was promptly removed following a valid takedown notice. These guarantees indisputably contributed to the rise of platforms like YouTube, Facebook, and other digital intermediaries by allowing them to host vast quantities of user-generated content without prior control—thereby laying the foundation for the global dominance of U.S. Big Tech in the digital economy.

Today, regarding AI regulation, U.S. companies once again hold a dominant position in the market, and policy is responding accordingly, with a push toward *non-regulation* rather than mere *deregulation*. A recent example is the attempt to introduce a ten-year moratorium on any state or local AI regulation, with the explicit goal of avoiding constraints on AI development and giving the industry a free hand to compete globally—particularly against China, a favorite target of Trump-era policies. This ban was included in the *Big Beautiful Bill* (H.R.1), a tax and infrastructure reconciliation bill, with strong backing from major tech firms who argued that a uniform federal framework would be more efficient than a fragmented patchwork of state laws[30].

This moratorium—applying to AI systems, algorithmic models, or automated decision-making tools—was meant not only to block new laws but also to nullify existing ones, effectively transferring all regulatory power to Congress. According to its proponents, this would reduce legal fragmentation among single states.

However, the proposal was overwhelmingly rejected by the Senate with a bipartisan 99-to-1 vote. It must be noted, though, that this outcome was less about a principled rejection of AI deregulation and more about a Republican inclination to

[29] See *Verbiest T., Spindler G., Riccio G.M.,* Study on the Liability of Internet Intermediaries, European Commission, DG Internal Market, 22007, SSRN: <https://ssrn.com/abstract=2575069 or http://dx.doi.org/10.2139/ssrn.2575069>, 2002, and more recently *Geiger C., Frosio G., Izyumenko E.,* The Oxford Handbook of Online Intermediary Liability, Oxford University Press, 2020.

[30] In particular, see the statements made by Sam Altman and reported by Tech Policy Press, *Transcript*: Sam Altman Testifies at US Senate Hearing on AI Competitiveness, https://www.techpolicy.press/transcript-sam-altman-testifies-at-us-senate-hearing-on-ai-competitiveness/. Specifically, the entrepreneur rejected proposals requiring developers to obtain government approval before releasing AI systems, calling them "disastrous" for the sector. He nonetheless emphasized that the establishment of standards by NIST (National Institute of Standards and Technology) could be useful, provided it does not slow down progress. Moreover, while acknowledging the United States' technological edge over China, he argued that this lead is difficult to assess from a forward-looking perspective. To reinforce this point, he concluded that the future of AI must be grounded in "democratic values such as transparency and freedom," setting itself apart from authoritarian models.

preserve the autonomy of individual states. In other words, the rejection reflected concerns over the federal-state relationship and administrative discretion, rather than an effort to prevent unregulated AI development.

Still, while this case does not demonstrate a clear stance on AI policy, it shows that the winds in U.S. regulation may be shifting.

As recently observed, the Biden administration's strategy unfolded in two phases[31]. The first, more programmatic phase included the publication of the *Blueprint for an AI Bill of Rights* in 2022—a non-binding document outlining core principles for responsible AI use: protection from surveillance, algorithmic transparency, non-discrimination, and accountability. The second, more operational phase came with *Executive Order 14110* of October 30, 2023[32], which imposed binding obligations on developers of advanced AI models, particularly dual-use systems, adopting a holistic approach that integrates national security, civil rights protection, and innovation promotion.

While this Executive Order did not create direct federal legislation, it outlined a detailed set of obligations, guidelines, and directives for federal agencies, aiming to balance technological innovation with national security and civil liberties. Several of its core principles aligned with those of the European *Artificial Intelligence Act*. For instance, the order mandated transparency obligations for companies developing high-impact foundation models—particularly those exceeding certain thresholds of computational capacity or trained on large datasets of non-public information. These thresholds were defined by the Department of Commerce, via the National Institute of Standards and Technology (NIST), in collaboration with other technical and security agencies.

Further parallels include obligations around transparency and combating deepfakes, involving experimentation with watermarking and content traceability technologies, the development of technical standards for identifying AI-generated content, and the creation of provenance protocols to strengthen public trust in digital information.

However, with Trump's return to the presidency in January 2025, there was a substantial shift in regulatory direction. This began with *Executive Order 14179*, which fully revoked Biden's order and directed federal agencies to review and eliminate regulations deemed to hinder AI development. Trump's approach, clearly grounded in deregulatory principles, seeks to reassert U.S. technological leadership by eliminating constraints perceived as ideological or anti-innovation—especially those aimed at addressing perceived "woke" or politically biased content in generative AI models[33].

[31] See *Lubello V.,* From Biden to Trump: Divergent and Convergent Policies in The Artificial Intelligence (AI) summer, in Bocconi Legal Studies Research Paper, 2025, SSRN: <https://ssrn.com/abstract=5302544>.

[32] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

[33] U.S. House of Representatives, Censorship's Next Frontier: The Federal Government's Attempt to Control Artificial Intelligence to Suppress Free Speech, Interim Staff Report of the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government U.S. House of Representatives, December 18, 2024.

4. On the Future Possible Circulation of the EU Legal Model

In recent decades, we have witnessed a profound transformation in the role of law (particularly private law) within the legal system, marked by a gradual loss of its centrality in favor of regulatory law and technical rules. This shift reflects not only an evolution in the forms of norm production but also a change in the very conception of law, increasingly seen as a functional tool for the economy rather than as an expression of general and structural principles intended to endure over time.

Classical private law, grounded in the 19th-century civil code model, was based on abstract, stable, and flexible categories designed to ensure legal certainty and to regulate interpersonal relationships in a systematic logic. However, in contemporary times, this framework has been progressively overshadowed by regulatory law—understood as a set of sector-specific rules, often of a public law nature, aimed at regulating specific areas of the economy (e.g., energy, telecommunications, finance, healthcare, environment) through targeted, contingent, and often technocratic interventions.

As leading scholars have observed, "private law has given way to a functional type of law, governed by independent authorities and efficiency logics, often disconnected from any systemic design." [34] These results in a form of "episodic" legislation, where overall coherence is sacrificed on the altar of political urgency, market pressure, or media contingencies. Legislators abandon the construction of durable, structural norms in favor of producing legal texts designed to address immediate problems, without any long-term vision.

Regulatory law represents the triumph of *governance by instruments*—as sharply noted—a form of public policy implemented through technical tools, bypassing political deliberation and democratic debate[35]. In this process, law tends to lose its ordering and predictive function, becoming a patchwork of special, heterogeneous rules lacking any systemic vision. The AI Act—despite laying down certain principles—is a prime example: a complex tangle of sectoral rules, often considered ill-suited even by technical experts and difficult to understand (and apply) for legal professionals.

In this context, the normative language itself is affected by the technocratic drift: norms are often written in hyper-detailed form, with continuous references to implementing regulations or technical standards, making them hard to understand not only for the average citizen but also for legal practitioners. This creates a deficit in accessibility and a disconnect between the law and its recipients, undermining the principle of substantive legality. A paradigmatic example is definition no. 67 in Article 3 of the AI Act, which defines "floating point operation" as "any mathematical operation or assignment involving floating point numbers, a subset of real numbers

[34] *Alpa G.,* Diritto privato e tecnica legislativa, 2018, see also *Micklitz H. W.,* Introduction, in Costitutionalization of European Private Law, Oxford, 2014, 1.
[35] *Lascoumes P., Le Gales P.* (éds.), Gouverner par les instruments, Science Po, Paris, 2005.

generally represented on computers using a fixed-precision integer with a scaling factor that is an integer exponent of a fixed base."

Some scholars have linked this transformation to the rise of the neoliberal paradigm, which has produced a vision of law as a technical instrument in the service of the market rather than as a vehicle for justice or social rebalancing—where the supposed "technical neutrality" of law is a myth: every regulatory choice affects power structures and reflects specific interests, and thus corresponds to a selection of which interests are to be protected over others[36].

However, this is not the only reason for the waning of the *Brussels Effect*. Another cause is the legislative "flood": Digital Services Act, Digital Markets Act, Artificial Intelligence Act, Cyber Resilience Act, Data Act, Data Governance Act—just to name a few. This massive production, often labeled as soft law but in practice binding, comes from administrative authorities both at the central and national levels. It exacerbates the risk of inconsistencies among legal texts, which are frequently the result of lobbying pressures and therefore poorly coordinated within a unified and coherent legislative vision[37].

This overproduction of norms, not matched by an equally robust technological development at the European level, creates paradoxical effects (e.g., the companies subjected to the first bans under Article 5 of the AI Act, in force since February 2025, are non-European). It also leads to differentiated business strategies, such as those adopted by some U.S. companies that have decided not to offer AI services within the European Union[38].

Moreover, as noted in the *Draghi Report* presented to the European Commission in late 2024, Europe has failed to foster companies with adequate technological capacity (and therefore comparable to U.S. and Chinese "giants") [39]. This results in Europe's total dependency on third-party actors[40]—a gap further amplified by slow decision-making processes, formalistic obligations (which are, not coincidentally, leading to revisions of the GDPR, starting with the elimination of the record-keeping requirement for SMEs) [41], and a limited ability to replicate virtuous practices in smaller or less technologically advanced Member States.

---

[36] *Purdy J.S., Grewal D.S., Kapczynski A., Sabeel Rahman K.,* note 23, 1791.

[37] Cf. *Padeiro P. J.F.*, Lobbying in the European Union's AI Act: the role of lobbying by the big five tech companies on the Council of EU's legislative process, Instituto Universitario de Lisboa, October 2024, 44; *Woll C., Artigas J.*, Big Tech's influence in the EU: Lobbying and digital governance, 61 European Journal of Political Research, 2022, 384; *Rozgonyi K.,* Digital giants and EU regulation: The lobbying strategies of Meta in Brussels, 19 Journal of Information Technology & Politics, 2022, 463.

[38] This is the case, for instance, of Apple: *Montgomery B.,* Apple delays launch of AI-powered features in Europe, blaming EU rules, The Guardian, 21 June 2024. Sharp tensions also arose in connection with the temporary suspension ordered by the Italian Data Protection Authority against OpenAI, the company behind ChatGPT. For further analysis on this case, see *Diurni A., Riccio G.M.,* ChatGPT: Challenges and Legal Issues in Advanced Conversational AI, in 9 The Italian Law Journal, 2023, 474.

[39] Cf. *Draghi M.,* The future of European competitiveness, European Commission, 2024.

[40] Some examples from the Draghi Report, including the one mentioned in the text of the article, had already been addressed, among others, by *Renda A.*, Beyond the Brussels Effect. Leveraging Digital Regulation for Strategic Autonomy, FEPS – Foundation for European Progressive Studies, Brussels, 2022.

[41] Press Agency, Targeted modifications of the GDPR: EDPB & EDPS welcome simplification of record keeping obligations and request further clarifications, 9 July 2025.

In conclusion, it is difficult to predict whether the European Union will be able to remain a beacon for the protection of fundamental rights in the context of AI development.

Some signals seem to point toward a decline in this influence and in the willingness of non-European companies—not only American ones—to adapt to European solutions. Consider, for instance, the response of the Chinese companies managing the large language model known as *DeepSeek*, who failed to respond to the requests of the Italian Data Protection Authority, apart from claiming that European privacy regulations did not apply to their activities[42]. An absurd response—it seems evident that the lawyers representing the Chinese companies could not have been unaware of the GDPR's scope of application—but one that nonetheless reveals a declining attractiveness of the European market for non-European AI companies.

In addition, perhaps this is the question we should return to: the European Union makes the rules, but are we still sure that the "innovator" countries are interested in following them?

Bibliography:

1. *Almada M.*, *Petit N.,* the EU AI Act: A Medley of Product Safety and Fundamental Rights. European University Institute, RSCAS Working Paper 2023/59, 2023.
2. *Alpa G.,* Diritto privato e tecnica legislativa, 2018.
3. *Ancel M.*, Utilità e metodi Del diritto comparato. Italian translation by P. Stanzione. Camerino, 1974.
4. *Ascarelli T.,* Premesse allo studio del diritto comparato, in Studi di diritto comparato e in tema di interpretazione, Milano, 1952.
5. *Bradford A.*, The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020.
6. *Calzada I.*, Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). Smart Cities 5: 1140, 2022
7. *Cannon R.,* The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway." Federal Communications Law Journal 49: 52, 1996.
8. *Costantinesco L.,* metodo comparative, Torino, 2000.
9. *Creemers R.,* China's Emerging Data Protection Framework, SSRN. https://ssrn.com/abstract=3964684, 2021.
10. *Creemers R., Webster G.,* (trans.), Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021), DigiChina, 2021.

[42] Garante per la protezione dei dati personali, Provv. January 30, 2025, doc. web n. 10098477.

https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

11. *Diurni A., Riccio, G. M.,* ChatGPT: Challenges and Legal Issues in Advanced Conversational AI, The Italian Law Journal 9: 474, 2023.
12. *Downes L.,* The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age, Basic Books, 2009.
13. *Draghi M.,* the Future of European Competitiveness. European Commission, 2024.
14. *Ferrajoli L.,* "Crisi del diritto e dei diritti nell'età della globalizzazione." Questione Giustizia. <https://www.questionegiustizia.it/articolo/crisi-del-diritto-e-dei-diritti-nell-eta-della-globalizzazione>, 2023.
15. *Geiger C., Frosio, G., Izyumenko E.,* the Oxford Handbook of Online Intermediary Liability. Oxford University Press, 2020.
16. *Gorla G.,* "Diritto comparato." Enciclopedia del diritto, XII, Milano, 1964.
17. *Grossi P.,* Aspetti giuridici della globalizzazione economica. In Atti della Accademia dei Georgofili, 2013.
18. *Hoecke M. Van*, ed. Epistemology and Methodology of Comparative Law. Hart Publishing, 2004.
19. *Imm M. R.,* Marketing Pornography on the Information Superhighway, Georgetown Law Journal 83: 1849, 1985.
20. *Kennedy D.,* Law-and-Economics from the Perspective of Critical Legal Studies. In The New Palgrave Dictionary of Economics and the Law, ed. *Newman P.,* London, <https://duncankennedy.net/wp-content/uploads/2024/01/law-and-economics-from-the-perspective-of-cls.pdf>, 2002.
21. *Lascoumes P*., *Le Galès P*., eds. Gouverner par les instruments. Sciences Po, Paris, 2005.
22. *Liz dos Santos A. L.,* Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais. Revista dos Tribunais 105, 2020.
23. *Lubello V.,* From Biden to Trump: Divergent and Convergent Policies in the Artificial Intelligence (AI) summer, Bocconi Legal Studies Research Paper. SSRN: https://ssrn.com/abstract=5302544, 2025.
24. *Major A. M.,* Internet Red Light District: A Domain Name Proposal for Regulatory Zoning of Obscene Content, Marshall Journal of Computer & Information Law 21, 1997.
25. *Mattei U.,* Comparative Law and Economics. University of Michigan Press, 1997.
26. *Meier P., Métille S.,* Loi fédérale sur la protection des données. Helbing Lichtenhahn Verlag, 2023.
27. *Montgomery B.,* Apple Delays Launch of AI-powered Features in Europe, Blaming EU Rules. The Guardian, June 21, 2024.
28. *Moriconi C.,* Recent Evolution of the Personal Privacy Legal Protection in People's Republic of China. Nordic Journal of Law and Social Research 9: 248, 2019.
29. *Pereira J. F.,* Lobbying in the European Union's AI Act: The Role of Lobbying by the Big Five Tech Companies. Instituto Universitário de Lisboa, 2024.

30. *Purdy J. S., Grewal D. S., Kapczynski A., Rahman S., K.,* Building a Law-and-Political-Economy Framework, Yale Law Journal 129: 1784, 2020.
31. *Renda A.* 2022. Beyond the Brussels Effect: Leveraging Digital Regulation for Strategic Autonomy. Foundation for European Progressive Studies (FEPS), Brussels.
32. *Richards N.,* Why Privacy Matters. Oxford University Press, 2021.
33. *Rozgonyi K.,* Digital Giants and EU Regulation: The Lobbying Strategies of Meta in Brussels, Journal of Information Technology & Politics 19: 463, 2022.
34. *Sacco R.,* Circolazione e mutazione dei modelli giuridici, In Digesto delle discipline privatistiche, sez. civ., II. Torino: UTET, 365, 1988.
35. *Sacco R.,* Introduzione al diritto comparato. Fifth ed., in Trattato di diritto comparato, Torino: UTET, 1992.
36. *Santoni G*., Personal Data as a Market Commodity: Legal Irritants from China's Experience, European Journal of Privacy Law and Technology 1, 2023.
37. *Stanzione P.,* Sui metodi del diritto comparato, Introduzione a *Ancel M.,* Utilità e metodi del diritto comparato, trad. it., Camerino, 1974.
38. United States Code, Title 18, Chapter 7, Title 47 § 223.
39. *Verbiest T., Spindler G., Riccio G. M.,* Study on the Liability of Internet Intermediaries. European Commission, DG Internal Market. SSRN: https://ssrn.com/abstract=2575069, 2002.
40. *Viola M., L. Heringer.,* Um olhar internacional: Lei Geral de Proteção de Dados Pessoais (LGPD) e o General Data Protection Regulation (GDPR), adequação e transparência internacional de dados, in Souza C.A., *Magrani E., Silva P.,* (eds.), Lei Geral de Proteção de Dados(LGPD): caderno especial, São Paulo, Thomson Reuter, 2019, 227.
41. *Voss W. G., Pernot-Leplay E.,* China Data Flows and Power in the Era of Chinese Big Tech, 44 Nw. J. Int'l L. & Bus. (2024) 1.
42. *Woll C., Artigas, J.* Big Tech's Influence in the EU: Lobbying and Digital Governance. European Journal of Political Research 61: 384, 2022.
43. *Zeno-Zencovich V.,* Comparison Involves Pluralism: A Rejected Viewpoint, Comparative Law Review 6, 2025.
44. *Zheng G.,* Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China, 43 Computer Law Security Rev. 105610, 2021.

Endre Győző Szabó*

From a Data Protection Authority to a Data Controller — Experiences within Eurostat**

Moving from a supervisory role to advising a data controller involves a shift in responsibility and perspective. When advising a data controller, further to general knowledge, the legal experts need sector-specific knowledge to advice data controllers effectively. Networking with other experts is crucial to ensure that high level of expertise is available.

Even if not expressly mandated, privacy professionals have a prominent role in building data protection culture in the given organization. This includes prominently raising awareness of data protection among staff members.

Statistical confidentiality naturally aligns with data protection needs. Successful enforcement involves constructive collaboration with respondents and feasible solutions.

The EU has introduced significant changes in the statistical framework in 2024 through the amendments to the Regulation on European statistics. In recent years, the emphasis shifted from survey data to administrative data and new technologies. Private data holders are obliged under the new framework to provide data for free to produce European statistics.

National Statistical Institutes and Eurostat can access personal data under strict conditions when requesting privately held data. This general provision needs to be complemented with a sectoral legislative act, listing the categories of personal data that may be accessed. When accessing and processing personal

* PhD, Legal and Policy Officer and Data Protection Coordinator of Eurostat.

** The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

data for statistical purposes, both GDPR and EU DPR continue to apply.

The essay concludes that privacy professionals are integral to their organizations, contributing to mission success. They suggest optimal, lawful adjustments whenever necessary and foster a data protection culture. Ensuring compliance and trust-building is fundamental in producing official statistics.

Keywords: *Privacy professionals, Data Protection Authority, National Statistical Institutes, statistics, data protection culture, privately held data*

1. Introduction

For me, the Spring Conference is not just one of the many events held in the field of data protection. It has a special place in my heart as I have attended many of these yearly gatherings and had the honour to host two Spring Conferences in Budapest, Hungary. First in 2016 and then in 2023. The latter event marked a closing moment of the first half of my career. In May 2023, I was still on the stage as part of the hosting team of the event, and in August same year, I opened a new chapter in my professional life and joined the European Commission, and more closely the Statistical Office of the European Union: Eurostat.[1]

Moving from the Data Protection Authority (DPA)[2] to a data controller is not only a significant move in a person's career but also has far-reaching implications in their daily work. More precisely, the perspective changes completely: the supervisory authority usually judges the lawfulness of a processing operation ex post, while within the data controller's organization the data protection specialist contributes to the decision-making process by advising the data controller. This is an utterly different form of responsibility, which, although based on the same foundations, fundamentally changes the logic and dynamics of one's work.

This is my personal journey that has been ongoing since 2023. I have attended the Spring Conference in Tbilisi, Georgia, with this background.

[1] Eurostat is based in Luxembourg; it is the statistical office of the European Union and at the same time a Directorate-General of the European Commission. The Luxembourgish National Commission for Data Protection (CNPD) hosted the Spring Conference back in 2012.

[2] The author had been working for the Data Protection Authority of Hungary for almost twenty years. He was the first Seconded National Expert in the offices of the European Data Protection Supervisory in 2006-2007. He had been the Vice-president of the Authority for Data Protection and Freedom of Information in Hungary between 2012 and 2023.

2. Getting Ready to Advise a Data Controller

Working for a data protection supervisory authority and being part of the network of the DPAs within the European Union is, obviously, an excellent environment for an expert before joining a data controller. Whilst the experts working for the DPA have a sound horizontal knowledge about data protection, it is not necessarily the case regarding familiarity with sectoral legal expertise needed in each possible specific field. Therefore, it is necessary to get acquainted with the sectoral legislation and also the "DNA" of the data controller. Without having an insight into the functioning and features of the controller, the data protection expert will not be able to provide helpful advice for the colleagues seeking guidance.

Similarly, to other colleagues, my experience also confirmed how important the availability of a network of experts in similar situation is. This is not only relevant for the first period of the work but remains important later as well, when dealing with difficult cases, for example the application of new technologies. A good network that is available for the expert is indispensable to ensure the quality of everyday work.

3. Cooperation with Staff Members in Implementing Data Protection Legislation – Building Data Protection Culture

It is crucial that staff members are well aware of data protection rules so that they can turn to the data protection expert for advice in good time. My experience within Eurostat confirmed that it is the case, and it is not by accident so, as statistical confidentiality is one of the guiding principles throughout the everyday work of statistical offices. Statistical confidentiality refers to the protection of data linked to so-called statistical units, like companies, households and natural persons as well. Therefore, the protection of data in general is a natural requirement in the statistical world. It has always been my experience that colleagues working in the statistical field can easily identify relevant issues and questions from data protection point of view.[3]

The culture of prudent approach is deeply rooted in statistical offices as they publish vast amount of information on a daily basis and the publication of confidential data has to be avoided by all means.

Let's also talk about challenges. Enforcing data protection requirements are not always popular but they are well understood and implemented if the colleagues are well trained. It is also important that the Data Protection Coordinator (DPC)[4] is constructive and is looking for alternatives and feasible solutions. This role cannot be an 'ivory tower stance', the DPC is part of the broader team and works for the success

[3] Statistical confidentiality means "the protection of confidential data related to single statistical units which are obtained directly for statistical purposes or indirectly from administrative or other sources and implying the prohibition of use for non-statistical purposes of the data obtained and of their unlawful disclosure" (Article 2 (1) e) of Regulation (EC) 223/2009 on European Statistics).

[4] Within the European Commission all Directorates-General have a Data Protection Coordinator (DPC). The Commission itself has a Data Protection Officer (DPO).

of the organisation. For me one of the key takeaways from the Budapest conference was what Anna Poliou, (shortlisted EDPS candidate in 2024), said. This is not a verbatim quote but still expresses the point: not saying *no* makes you a good privacy expert, but your ability to assist your organisation in *how* to achieve the goals in a manner that is lawful and compatible with privacy legislation.

Cooperation with colleagues on a regular basis, providing training for newcomers, assisting data controllers when assessing data protection related questions – this all contributes to an endeavour to nurture the data protection culture within the organisation. This culture might seem invisible for some time, the presence of a good data protection culture will though become clearly tangible when dealing with cases, especially complex cases.

4. The World of Statistics – Major Changes in the Framework Regulation

The framework Regulation on European statistics went through a significant amendment in 2024. The main goals behind the amendment are, first of all, to adjust statistical production to the state of the art and to harvest what is available in terms of new technologies and new data sources. This implies tapping the full potential of digital data sources and new technologies. In addition, the amendments aim to improve statistics and the functioning of the European Statistical System,[5] in other words, to become more pro-active and produce statistics more efficiently. Finally, the framework will help to innovate statistical production and the development of new statistics.

5. Shift from Survey Data to Administrative Date Sources

In recent years, we are witnessing a clear shift from survey data to administrative data used for statistical production. You may still encounter surveys, like in the field of statistics of income and living conditions (SILC), where selected respondents are interviewed. But the main source is getting more and more administrative registers.

As the technological environment is changing and sharing of information is speeding up, there is a constant need to streamline statistical production to provide more timely, more precise, high-quality statistics.

[5] According to Article 4 of the Regulation (EC) 223/2009 on European Statistics, „The European Statistical System (ESS) is the partnership between the Community statistical authority, which is the Commission (Eurostat), and the national statistical institutes (NSIs) and other national authorities responsible in each Member State for the development, production and dissemination of European statistics".

6. Access to Privately Held Data

Private data holders are in possession of highly valuable data sets, let it be data related to bank card use, smart meters, mobile network operators, logistical companies, just to mention a few.

A new and general obligation has been imposed on private data holders by the amended framework regulation: private date holders are obliged to make data and relevant metadata available free of charge where the data is strictly necessary for the development, production and dissemination of European statistics, and cannot be obtained by other means, or, alternatively, the reuse of privately held data will result in a considerable reduction in response burden.[6] This is an enormous change in statistical production and a long-awaited chance to better serve the decision makers with timely and high-quality statistics, which is the ultimate goal of European statistics and statistics in general.

7. Access to Personal Data among Privately Held Data

The co-legislators equipped the National Statistical Institutes and Eurostat with new and strong rights, meaning that they can have access, under strict conditions, to personal data among privately held data. The data minimisation and proportionality principle apply for data requests in general. In line with these principles, when it comes to access to data, as a main rule, only non-personal data may be requested.

In specific circumstances the list of personal data may be specified in sectoral legislation. This means that the amended framework legislation on European statistics is not a sufficient basis in itself to request personal data. It needs to be supplemented and further specified in another legislative act.

The Regulation on European Union labour market statistics on businesses (LMB)[7] is the first sectoral legislation adopted after the Regulation on European Statistics was amended in 2024. This regulation specifies that any such request shall be limited to the personal data categories covered by the domains and topics specified in that Regulation.[8] This provision also sets the limits of the personal data that can be requested from private data holders.

As this is still new set of rules and therefore no use cases can be presented in this essay, we have to limit our analysis to existing rules, waiting for future

[6] According to Article 17b (1) of Regulation (EC) 223/2009 on European statistics, „…an NSI or the Commission (Eurostat) may request a private data holder to make data and the relevant metadata available free of charge where the data requested are strictly necessary for the development, production and dissemination of European statistics and cannot be obtained by other means or their reuse will result in a considerable reduction in the response burden on data holders and other businesses. Such data collections or data access may be included by the Commission in the annual work programme".

[7] The Regulation (EU) 2025/941 of the European Parliament and of the Council of 7 May 2025 on European Union labour market statistics on businesses is applicable from 1 January 2026.

[8] More specifically, the list of possible data that can be requested is listed in Article 4 of the Regulation. According to Article 3 (3), „request shall be limited to the personal data categories covered by the domains and topics specified in Article 4 of this Regulation".

implementation. In case of access, the entire data protection regime is, of course, applicable – at Member State level the GDPR[9], at European Union level, for Eurostat, the so-called EUDPR.[10] Data Protection Officers in each National Statistical Institutes and the Data Protection Coordinator within Eurostat will follow these requests and will be available for advice for their respective data controllers.

Access to data has always been based on close cooperation between statistical offices and data holders, with the attempt to limit the burden on respondents to the extent possible. This can be expected under the amended framework as well, and further to applying the restrictions on access to data and personal data, maintaining good cooperation with data holders will remain a cornerstone of the implementation of the new rules.

For statistical authorities, statistical confidentiality is not just an aspect of compliance. They put in place all the necessary technical and administrative measures to ensure the protection of confidential data, including personal data. Further to compliance, this is also part of trust building towards respondents.

This consideration reminds me of Giovanni Buttarelli, late EDPS, and his memorable statement. During the Global Privacy Assembly back in 2018 in Brussels in the European Parliament building, Giovanni Buttarelli said: "*For me, compliance with the law is not enough*".[11] This is very true and relevant in the context of producing official statistics. Further to compliance and demonstrating compliance, trust building remains an important task for statistical institutes.

8. Conclusion

Based on the above analysis and my experience gained in my new role, some conclusions can be drawn. First, privacy professionals are not outsiders, but insiders, they are integral part of the organisation, and they can contribute to the success of the data controller's main mission.

Second, privacy professionals must remain available to propose optimal and lawful solutions if there is a need for adjustment, rather than simply advise against or excluding possible solutions. They should take, whenever possible, a constructive stance to assist their respective controller in achieving their main goals. If successful, this work will go hand in hand with the establishment of data protection culture within the organisation.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[10] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[11] The speech is available online: <https://www.youtube.com/watch?v=2gG1kY0L3a0>.

Finally, privacy professionals can contribute to the trust building by ensuring and demonstrating compliance and have the capacity to act as a sort of ambassadors of their employers to the outside world.

Bibliography:

1. Regulation (EC) No 223/2009 on European Statistics “The European Statistical System (ESS) “.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
3. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
4. Regulation (EU) 2025/941 of the European Parliament and of the Council of 7 May 2025 on European Union labour market statistics on businesses is applicable from 1 January 2026.
5. *Buttarelli G.,* Speech: Choose Humanity: Putting Dignity back into Digital, speech by Giovanni Buttarelli <https://www.youtube.com/watch?v=2gG1kY0L3a0>.

Júlia Sziklay*

The European Health Data Space (EHDS)**

The European Health Data Space (EHDS) regulation was accepted on 11 February 2025, the full applicability will be achieved from 26 March 2031. The Regulation has double aims, firstly to improve the patients' access to and control over their personal electronic health data in the context of healthcare and secondly to better achieve other purposes that would benefit society, such as to support research, patient safety, personalised medicine, health threats (including pandemics), innovation, policymaking, official statistics or regulatory activities. The EHDS is the first EU common dataspace with many promises, expectations and challenges.

Keywords: *European Health Data Space, EHDS, health data, data law.*

1. Introduction

Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (EHDS Regulation) aims to optimise the exchange of and access to health information within the EU.

The European Health Data Space (EHDS) represents the first common EU data space initiative as part of the broader European data strategy aiming to meet the needs of a data-driven economy. The goal is to promote the secure and trustworthy use and sharing of data across 14 key sectors, including agriculture, energy, transport, and finance. According to the official announcement *„The EU will become an attractive, secure and dynamic data economy by setting clear and fair rules on access*

* Vice President of International Affairs, National Authority for Data Protection and Freedom of Information (Naih).

** The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

and re-use of data; investing in next generation tools and infrastructures to store and process data; joining forces in European cloud capacity; pooling European data in key sectors, with common and interoperable data spaces and giving users rights, tools and skills to stay in full control of their data."[1]

The (re)use of personal data stored by public sector entities is only allowed under strict guarantees under EU data laws, which all follow an "access-based" approach, exemplified by horizontal regulations such as the Data Governance Act (DGA), Data Act (DA), and the Public Sector Information Directive (PSI). Anonymization is the general rule, and reidentification is explicitly prohibited by law. Furthermore, new rules have been introduced concerning non-personal data and the protection of the interests of legal persons. Neutral data intermediation services under the DGA aim to facilitate commercial relationships between data subjects, data holders, and users (for-profit). In parallel, altruistic data-sharing organizations, operating on a cost-recovery and nonprofit basis, support the voluntary, free-of-charge sharing of personal and non-personal data for public interest purposes. However, respecting the already existing horizontal EU legislation the EHDS introduces new sector-specific and *lex specialis* rules.

2. Dual Objectives of EHDS

1. Primary Data Use: Patients will have reinforced data protection rights in particular the right to access, to data portability, and to control over their personal electronic health data.

This includes:

- Adding personal health information;
- Restricting access to specific parts or individuals;
- Viewing access history;
- Requesting corrections in case of errors;
- Accessing their health data in a standardized European format.

2. Secondary Data Use: Electronic health data may also be used for broader societal goals such as:

- Research and innovation;
- Policy-making;
- Public health preparedness and response (including pandemics);
- Official statistics;
- Regulatory activities;
- Patient safety;
- Personalized medicine.

[1] European Commission, European Data Strategy, Making the EU a Role Model for a Society Empowered by Data, <commission.europa.eu/strategy-and-policy/priorities-2019-2024> [25.06.2025].

3. Implementation Timelines

2027:

- Member States must establish digital health and health access authorities and national contact points.

2029:

- Key EHDS services must be operational.
- Patients must have access to the first three data categories (medical history, e-prescriptions, e-dispensation).
- EHR systems must comply with EHDS specifications.
- Data users can submit applications for certain categories.
- Data holders must submit dataset descriptions to the access-granting authority.

2031:

- All EHDS services must be fully operational.
- Patients must have access to all their data.
- Marketed EHR systems must comply with EHDS specifications across all categories.
- Data users can apply for all data categories.
- Data holders must provide dataset descriptions.

4. Third countries

According to Preamble 35, the EHDS also supports exchanges of personal electronic health data with national contact points for digital health of relevant third countries and systems established at international level by international organisations in order to contribute to the continuity of healthcare. This is particularly relevant for individuals travelling to and from neighbouring third countries, candidate countries, and the associated overseas countries and territories. The connection of such national contact points for digital health of third countries to MyHealth@EU and the interoperability with digital systems established at international level by international organisations should be subject to a compliance check of the European Commission ensuring the compliance of those contact points and digital systems with the technical specifications, data protection rules and other requirements of MyHealth@EU. In addition, given that the connection to MyHealth@EU will entail transfers of personal electronic health data to third countries, such as sharing a patient summary when the patient seeks care in that third country, relevant transfer instruments under Chapter V of Regulation (EU) 2016/679 should be put in place. The Commission should be empowered to adopt implementing acts to facilitate the connection of such national contact points for digital health of third countries and systems established at international level by international organisations to MyHealth@EU. When preparing

those implementing acts, the Commission should take into account Member States' national security interests.

For secondary use, following assessment and joining HealthData@EU, access is only available from 2035 onward.

5. Data Categories and Sources

From the healthcare system:

- Admission documents, medical records, referrals;
- Biological samples, imaging, sensory and metadata;
- Prescriptions, predictive/personalized medicine data;
- Monitoring and control data.

From researchers and industry:

- Aggregated database analyses;
- Exploratory datasets;
- Case studies, biological sample analysis.

6. Opt-Out Rights

Except where vital interests must be protected, Member States may allow patients to opt out of data access:

- By healthcare professionals (primary use);
- Or further reuse (secondary use).

However, public interest use, policy-making, statistical, and research access are excluded from opt-out options.

7. Prohibited Secondary Uses

According to Article 54 of the EHDS regulation health data users may only process data in line with the purposes authorized in the:

- Data permit under Article 68;
- Approved data application under Article 69;
- Specific cases under Article 67(3) or approval under Article 75.

It is forbidden to use the data for:

- Making disadvantageous decisions based on electronic health data (e.g., with legal, economic, or social impacts);
- Employment or service-related discrimination (e.g., insurance, credit exclusions);
- Advertising or marketing;
- Developing harmful or addictive products (e.g., drugs, alcohol, tobacco, weapons);

- Activities violating ethical norms defined by national laws.

8. Governance Structure of the EHDS

Infrastructure includes:

- The already existing MyHealth@EU and HealthData@EU infrastructures;
- National contact points;
- Digital health authorities;
- Data access-granting bodies (to authorize access, to supervise compliance, to impose sanctions, biannual reporting);
- Market surveillance authorities (to supervise electronic health record sytems);
- The EHDS Board (shall be composed of two representatives per Member State, namely one representative for primary use purposes and one for secondary use purposes, nominated by each Member State; each Member State shall have one vote)
- Data holders and users.

9. Data Protection and Processing Principles Apply

The purpose of data processing standards is to protect fundamental human rights, not to alter or hinder sector-specific legal or professional practices. Processing must meet the standards of necessity and proportionality. The objective must justify the intrusion into privacy; "more effective medication" does not justify "more invasive development methods."

- Risk-based approach**:** Protection levels must correspond to the risks to individuals.
- Compliance: If the main process is non-compliant, the data processing cannot be compliant.
- Primary processing typically involves personal and identifiable data.
- Secondary processing requires access approval and typically involves anonymized or pseudonymized data.
- Anonymization is considered processing (requiring a legal basis), but once completed, the data is no longer considered personal data and falls outside the GDPR's scope.

Data protection authorities must be informed about imposed sanctions of the health data authorities and issues related to secondary data processing, and they should share relevant information to ensure rule enforcement.

10. Conclusion

The EHDS enables individuals to access, control, and share their electronic health data across borders, improving healthcare safety and patients' comfort. It also allows for the secure reuse of health data in research, innovation, policymaking, and regulatory activities. According to the European Commission, this could save up to €11 billion[2] in the EU over the next decade. Additionally, the EHDS supports the development of a single market for secure electronic health record systems that serve both primary and secondary uses.

On the other hand, due to its complexity and size the new infrastructures significantly raise the level of data protection risks in the form of various threats, including cyberattacks, insider threats, and data breaches. All these threats and injuries can lead to unauthorized access, loss of control, and great potential harm to individuals. These risks are further complicated by the sensitive nature of health data.

Bibliography:

1. European Commission, European Data Strategy, Making the EU a Role Model for a Society Empowered by Data, <commission.europa.eu/strategy-and-policy/priorities-2019-2024> [25.06.2025].
2. European Commission, Questions and answers - EU Health: European Health Data Space (EHDS), <ec.europa.eu/commission/presscorner> [25.06.2025].

[2] European Commission, Questions and answers - EU Health: European Health Data Space (EHDS), <ec.europa.eu/commission/presscorner> [25.06.2025].

Tamar Samniashvili*

Data Subject Consent as a Legal Basis: Theoretical and Practical Perspectives

The article discusses the data subject consent institution as a legal basis for the processing of personal data. It analyzes the criteria of lawful consent, including voluntariness, active expression of will, specificity, and clarity. The particular importance of consent in the processing of children's personal data and special category data is emphasized. The study examines the peculiarities of consent formulation in documents, contracts, and online environments, emphasizing the mandatory protection of transparency and informed consent principles.

The article is based on a comparative analysis of Georgian national legislation and international law, particularly the European Union's General Data Protection Regulation (GDPR).[1] Key challenges and risks in the practical implementation of the consent institution are identified.

The article presents the criteria necessary for the effective functioning of consent, whose implementation in practice contributes to the development of a data protection culture and the strengthening of public trust in both private and public sectors.

Keywords: *personal data, special category data, personal data of a child, consent, child's consent, right to withdraw consent, consent in a contract, consent in the online environment, pre-existing records ("cookie files"), General Data Protection Regulation (GDPR)*

* Master of Law, Ilia State University; Data Protection Officer at the LEPL – National Archives of Georgia.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016 (შემდგომში — GDPR)

1. Introduction

The consent of the data subject as a legal basis for the processing of personal data is provided for by the Law of Georgia on Personal Data Protection.[2] The issue that a data controller requires a legal basis for processing personal data is not new. Alongside the growing legal awareness of society, there is an increase, on the one hand, in the expectations and demands of data subjects, and on the other hand, in the obligations of data controllers to process data in accordance with the law.

Consent, as a legal basis for the processing of personal data, represents one of the most frequently used and relevant issues in practice. However, the Swedish Authority for Privacy Protection notes, when discussing the issue of consent, that: "consent is normally not the easiest nor the most appropriate alternative, for example because the person who gives their consent can revoke it at any time."[3]

In most cases, data controllers use this basis to bring existing or planned processes into compliance with the law. Specifically, in cases where no other legal basis for processing exists, the data controller establishes a legal basis for the process by obtaining consent. In such cases, there is a risk that consent may become a "universal instrument" allowing controllers to merely formalize processes within a legal framework. Accordingly, the risks associated with obtaining and subsequently implementing this legal basis should not be overlooked.

The Information Commissioner's Office (ICO) provides guidance on consent, according to which, for a specific processing activity, the lawful basis that most accurately reflects the purpose of the processing and the actual relationship with the data subject should be chosen."If consent is difficult, this is often because another lawful basis is more appropriate, so you should consider the alternatives".[4]

The importance of consent becomes even more apparent in the modern digital reality. In the era of Internet services, social networks, mobile applications, and digital marketing, the vast majority of data processing is based precisely on consent. Users press the "I agree" buttons daily, yet in reality, they rarely have the time or opportunity to fully understand what this consent entails and how genuinely free their choice is. Therefore, in recent years, discussions about the problem of "formal consent" and its effectiveness have intensified.

The use of consent in practice is particularly relevant in the private sector, where it is often associated with direct marketing, employment processes, insurance and banking services, and data processing in the education and healthcare sectors. In the public sector, the use of consent is comparatively limited, since data processing in these cases is mostly based on legally established obligations or public interest. In such

[2] Law of Georgia on Personal Data Protection 14/06/2023, Article 5(1)(a).

[3] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 15, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].

[4] *Information Commissioner's Office (ICO)* Guideline on *When is consent appropriate?* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/> [27.11.2025].

cases, the issue of voluntariness is particularly sensitive, as citizens often cannot perceive consent as a free choice in their interactions with public institutions. Therefore, in most cases, public authorities cannot rely on the consent of the data subject, considering the balance of power between the data subject and the data controller.[5]

The aim of the article is not only to provide a theoretical analysis of consent as a legal basis for data processing but also to highlight its practical significance, associated risks, and development perspectives.

2. Processing of Personal Data on the Basis of Consent

The Law of Georgia on Personal Data Protection defines the concept of consent and specifies the mandatory criteria for considering this legal basis as lawful:[6]

- **After receiving information** – consent must not be given in advance; it must be provided after the data subject has been informed about the matter for which consent is requested. This ensures, in turn, the possibility of a genuine choice.
- **Informed** – data controllers must ensure that clear and simple language is used for information purposes. The text must be easily understandable to any individual, not only to legal professionals, and must not include long, complex privacy policies or rules presented exclusively in legal terminology. The consent request must be distinct from other matters and communicated in plain, comprehensible language.
- **Specific purpose** – this criterion is directly linked to the requirement for adequate information. The data subject must be aware of the precise purpose for which their personal data is being processed and what they are consenting to.
- **Active engagement** – consent must be actively expressed by the data subject. In practice, this may take the form of marking a consent box in the presence of a written document, providing consent via a hyperlink, giving verbal consent, or another appropriate method.
- **Freely given** – consent must be voluntary, meaning the data subject must be able to make a decision regarding the processing of their personal data independently and without any pressure.
- **Unambiguous** – the data subject's intent regarding specific data and its specific processing must be clear and must not give rise to doubt regarding its existence.

[5] Guideline Recommendation of the Personal Data Protection Service of Georgia on "Obtaining Consent from the Data Subject", 10.
[6] Law of Georgia on Personal Data Protection 14/06/2023, Article 3(m).

- **Form** – consent may be provided in writing (including electronically) or verbally, depending primarily on the category of data for which consent is given. Specifically, for special categories of data, consent can only be given in written form.[7] The Law also provides similar specific regulation for direct marketing when processing data other than name, surname, address, telephone number, and email address.[8]

Notice and consent requirements often create the illusion, but not the reality, of meaningful consumer choice.[9] At the stage of assessing the lawfulness of consent, it is crucial that all the above criteria are fully satisfied.

3. Consent in Practice

Cases where consent is considered a lawful basis for data processing are primarily encountered in the private sector. The main reason for this is that in the public sector, it is rarely possible to imagine a specific situation in which consent requested by a public sector would not be perceived by the data subject as having a compulsory nature, taking into account both direct and indirect influence and the anticipated impact of the data controller.

A similar risk may exist regarding the lawfulness of the data subject's consent when the data subject is an employee and the processing is carried out by the employer. In this case, the subordinate position is evident, and accordingly, there is a real risk that the data subject's decision regarding a particular process may be associated with certain pressure and may negatively affect their expressed will and attitude.

However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.[10]

When requesting consent, data controllers have considerable leverage, the unlawful formulation and "covert" nature of which, even when brought to the attention of the data subject, may result in the obtained consent lacking legal effect. In such cases, it may be determined that the data controller actually carried out the specific data processing without a lawful basis.

[7] Ibid, Article 6(1)(a).
[8] Ibid, Article 12(2).
[9] *Cate, F. H.* The Failure of Fair Information Practice Principles In *Consumer Protection in the Age of the Information Economy,* 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].
[10] *European Data Protection Board (EDPB),* Guidelines on consent under Regulation 2016/679,2018, 7, <https://www.edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf> [27.11.2025].

It is important to emphasize, that: "If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis."[11]

Of course, this excludes situations in which the data controller seeks a lawful basis for the processing and considers the data subject's consent in their actions, such as silence, inaction, pre-ticked boxes, or the blanket acceptance of initial settings, rules, and terms and conditions.

It is often argued that treating the data subject's consent as a lawful basis for data processing may pose legal and practical risks. These risks may occur even if the data controller provides full information. In his work "The Practical Failure of Fair Information Principles," American data protection and privacy expert Fred H. Cate identifies one of the main difficulties in implementing information provision in practice: the general public's disregard for provided privacy policies and information. As data protection laws and regulations become more complex, the notices required by those enactments also increase in complexity.[12]

Similar risks are also addressed by the European Data Protection Board (EDPB) in its guidelines on consent, which note the dangers that arise when data subjects frequently provide consent without being adequately informed of the forms used to obtain it. As a result, a real risk is created for them, since consent is often requested for processing activities that would not be lawful without the expression of their explicit will.[13]

These circumstances, in turn, increase the risks associated with the lawfulness of consent.

3.1. Consent of a Child

The importance of lawful processing of a child's data is also evidenced by its regulation under special rules. Under Georgia's national legislation, as well as international standards, particular attention is paid to protecting the rights of a child and implementing effective mechanisms for their realization. This is primarily due to the inherent characteristics of children themselves, including their potentially incomplete understanding of the issue, inability to fully assess their best interests, and inability to fully perceive associated risks, which constitute a non-exhaustive list of circumstances that justify a high standard of protection for their rights.

[11] *"EDPB",* Guidelines 05/2020 on consent under Regulation 2016/679, 10, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

[12] *Cate, F. H.* The Failure of Fair Information Practice Principles In Consumer Protection in the Age of the Information Economy, 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].

[13] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

The Swedish Authority for Privacy Protection places particular emphasis on the protection of children's rights in the online environment. "Children and young people move quickly and expertly between various platforms, but this does not always mean that they realise the risks or understand the consequences – consequences that may be far away in the future."[14]

When obtaining consent from a child, the data controller must exercise particular care to ensure that the consent request is presented in a simple, comprehensible language suitable for a child, and, if necessary, supplemented with additional visual aids.[15] The Data Protection Commission (DPC) also discusses several examples of such measures: cartoons, videos, pictures, images, and game-related elements—adapted to the age groups of users—and considers them effective means of conveying information to children.[16]

The Law of Georgia on Personal Data Protection also provides for a different regulatory approach when it comes to special category data of a child.[17] In such cases, in addition to the high risk associated with children, the characteristics of the data itself require a high standard of protection. Specifically, processing special category data of a child is permissible under the law only with the written consent of the parent or legal guardian, unless otherwise provided by law.[18]

3.1.1. Consent of a Child – International and National Practice

The European Union's General Data Protection Regulation (GDPR), as well as Georgia's national legislation, provides for special regulation regarding the processing of a child's data. Specifically, in these cases, the relevant threshold age is considered to be 16 years, at which point the data subject is granted the right to manage their personal data and consent to specific processing activities.[19] For a full understanding, it should be noted that there are exceptions to this rule where the law directly specifies a different regulatory approach.[20]

Additionally, Georgia's legislation imposes strict requirements to ensure a high standard of protection when processing children's data, setting the minimum age for

[14] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 3, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[15] *The Autoriteit Persoonsgegevens (AP),* Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent> [27.11.2025].
[16] *Data Protection Commission (DPC),* Fundamentals for Child-Oriented Approach to Data Processing, December 2021,29, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [27.11.2025].
[17] Law of Georgia on Personal Data Protection 14/06/2023, Article 7(3).
[18] Ibid., Article 7(1).
[19] GDPR, Article 8 (1)
[20] Law of Georgia on Personal Data Protection 14/06/2023, Article 7(1).

giving consent to data processing at 16,[21] whereas Article 8 of the EU General Data Protection Regulation (GDPR) allows member states to set the minimum age at no less than 13 years.[22] This difference reflects Georgia's inclination to maintain a stricter standard for the protection of children's data.

In contrast to this approach, the United Kingdom's UK General Data Protection Regulation (UK GDPR) adopts a more flexible regulatory approach, establishing that the minimum age for giving consent to the processing of a child's data is 13 years.[23]

In the guide "The rights of children and young people on digital platforms" Swedish Authority for Privacy Protection notes, when discussing consent given by persons aged 13 to 16, that: "it needs to be assessed in each individual situation if the child in question can be considered able to understand the consequences of consent. Factors influencing this assessment include how sensitive the personal data provided by the child are, how long they will be saved, as well as the age and maturity of the child."[24]

The French data protection authority (CNIL — Commission nationale de l'informatique et des libertés), when addressing the protection of child's personal data, also emphasizes the importance of parental control mechanisms."Children are not necessarily able to fully understand the risks they face online and make informed decisions. Parents need effective tools to support them in their online lives."[25] However, attention is also drawn to the need for caution to ensure that the control mechanism is not excessively intrusive, so that its use does not lead the children to feel under constant supervision.[26]

The French data protection authority's (CNIL) recommendation also defines the need for parental control mechanisms to comply with data protection regulations. "Any proposed parental controls must comply with data protection rules, and in particular with:

- The **principle of proportionality** taking into account the child's interests, age and level of maturity, and avoiding the use of intrusive features such as constant tracking;
- The **principle of transparency** towards the child by clearly explaining which parental controls are being used;

[21] Ibid.
[22] GDPR, Article 8 (1).
[23] UK General Data Protection Regulation (UK GDPR), Article 8 (1).
[24] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 20, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[25] *CNIL (Commission nationale de l'informatique et des libertés), Recommendation 5: Promote parental controls that respect the child's privacy and best interests,* 09 August 2021. <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
[26] Ibid.

- The **principle of security** of the child's data, in order to ensure that third parties do not have access to information about the child (e.g. the child's geolocation data). "[27]

When discussing the issue of parental/guardian control over children, the Swedish Authority for Privacy Protection notes that they must not be subjected to unlawful or arbitrary restrictions on their personal and family lives. Those exercising control bear responsibility for the child's upbringing and development, taking into account the child's best interests. In this context, a particularly important task is to balance the existing interests and to be aware of their significance.[28]
"The older the child is, the greater consideration must be given to the child's own will and consent"[29].

3.2. Consent in a Document Regulating Multiple Issues

When selecting the data subject's consent as the legal basis for data processing, the data controller must exercise particular care and attention when consent is included as part of a document that, in addition to the mentioned matter, also regulates other issues.

In this case, it is particularly important that the consent text in the relevant document is formulated clearly, in simple and understandable language, and also separated from other parts of the document.[30]

A similar requirement is provided in the European Union General Data Protection Regulation (GDPR)**,** specifically Article 7(2): "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."[31]

This requirement is based on the principle of transparency in data processing. The data subject must clearly understand exactly which processing activities they are consenting to, which data will be processed, for what purpose, and on what legal basis. Any consent form that is not visible, not separated from the full text of the document, and, by reasonable assessment, is not perceived as a choice given by the data subject regarding the management of their personal data, must be excluded**.** Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

[27] *CNIL (Commission nationale de l'informatique et des libertés), Recommendation 5: Promote parental controls that respect the child's privacy and best interests,* 09 August 2021, <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
[28] *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 40, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
[29] Ibid.
[30] Law of Georgia on Personal Data Protection 14/06/2023, Article 32(1).
[31] GDPR, Article 7 (2).

3.3. Consent in a Contract

The principle of transparency is particularly important when the document through which the data subject's consent is obtained constitutes a contract.

In this context, the voluntariness of consent is especially sensitive. Consent included in a contract must ensure that the data subject can freely exercise their will, make an informed choice, and that their decision does not affect the terms of the contract, including the decision to enter into or refrain from entering into the contract.

When consent is given in the context of a contract or the provision of a service, the assessment of voluntariness must take into account, among other factors, whether consent is a necessary prerequisite for the contract or service, and whether the contract or service can be provided without such consent.[32]

This regulation corresponds to the approach of the European Union General Data Protection Regulation (GDPR), which emphasizes that when giving consent for data processing, the data subject's will must be clearly expressed, and that it must not cover data processing that is not necessary for the performance of the contract.[33]

3.4. Consent in the Online Environment

In parallel with the ongoing digitalization of today's reality and the growing use of online services, the number of risks associated with consent obtained from the data subject for the processing of personal data on online platforms is also increasing. The legality of consent obtained through websites, mobile applications, and online services constitutes one of the most relevant and problematic issues.

The European Data Protection Board (EDPB), in its guidelines on consent, addresses the specificities of the digital environment and the associated risks. In particular, in online contexts, data subjects are routinely confronted with numerous consent requests, often expressed through the ticking of buttons or clicking of links. The frequency of such actions may result in a habituation effect, whereby the data subject's vigilance and attentiveness are reduced due to excessive interaction with consent mechanisms. Consequently, there is a real risk that consent may be provided without full awareness, particularly where it is requested for processing activities that would not otherwise be lawful without the data subject's explicit expression of will.[34]

Despite the fact that even in the online environment it is mandatory to comply with legally established criteria and requirements for consent, in practice, there are frequent cases where the form of requesting consent is purely formal. This harmful

[32] Personal Data Protection Service of Georgia, Guideline Recommendation on "Obtaining Consent from the Data Subject," 21.
[33] GDPR, Article 7 (4).
[34] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].

practice is especially common regarding the regulation of pre-existing records "cookie files" on websites. Upon visiting a website, joint consent forms for existing cookies are often presented, whereas the data subject has the right to make a choice and consent to the processing of their data only for those cookies they desire, or for cookies that are necessary for the functioning and security of the website, and therefore are essential for its operation.

Furthermore, it is important that consent is obtained upon entry to the website**,** before cookies or other data are placed on the user's device, for example through cookie banners. Consent must be separate for each purpose of data processing (e.g., advertising, analytics, etc.), and the data subject must provide it individually**.**[35]

In addition, the legally defined criteria for consent acquire particular importance in the online environment. In particular, the principles of transparency and informed consent require that the information provided to the data subject be clear, understandable, and specific.

In the context of online consent, an interesting discussion can be found in one of the decisions of the Court of Justice of the European Union (CJEU) in Planet49 GmbH (C-673/17, 1 October 2019)**,** which states that in such cases:" it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not deselecting a pre-ticked checkbox nor, in any event, whether that consent had been informed. It is not inconceivable that a user would not have read the information accompanying the preselected checkbox, or even would not have noticed that checkbox, before continuing with his or her activity on the website visited"[36]

Consent obtained in the online environment must itself be obtained through active action (clicking a button, checking a box, etc.), which excludes the legal validity of consent obtained through pre-checked or automatically selected forms**.**

3.5. Right to Withdraw Consent

One of the guarantees of the voluntary nature of consent is also the possibility to freely withdraw consent and the provision of information to data subjects about this right. Similar to the provision of information on data processing in advance, information regarding the withdrawal of consent must also be provided prior to the data subject giving consent**.**

The regulation of the right to withdraw consent is addressed in several provisions of the Law of Georgia on Personal Data Protection**.**

Direct Marketing – Article 12 of the Law of Georgia on Personal Data Protection[37] establishes the obligation to provide information on the right to withdraw consent and

[35] Personal Data Protection Service of Georgia, "Guide for Individuals Interested in Creating a Website", 27.
[36]European Court of Justice, CJEU, Case C-673/17, Planet49 GmbH [2019], §55, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143828> [27.11.2025].
[37] Law of Georgia on Personal Data Protection 14/06/2023, Article 12(3).

the guarantees for the exercise of this right, specifically in terms of its free of charge and unrestricted use.

Chapter on Data Subject Rights – Article 20 of the Law of Georgia on Personal Data Protection[38] details the necessary preconditions for the exercise of this right:

- **Without temporal limitation, at any time** – this excludes the possibility for the data controller to set any specific time frame for requesting consent, even by specifying and justifying their particular purpose.
- **Without explanation or justification** – to implement effective measures for the realization of the purposes of the law and the fundamental rights of the data subject, it is important to guarantee the possibility to withdraw consent without providing justification or explanation.
- **Using the same means by which consent was given** – the criterion of voluntariness and free exercise of will implies that the data controller must not apply any influence, pressure, or obstacles that would artificially prevent the exercise of this right, and must ensure that consent can be withdrawn in the same manner it was given.

Moreover, when assessing the lawfulness of consent, the burden lies with the data controller to demonstrate that the exercise of this right by the data subjects is not associated with any particular costs and, accordingly, does not entail an obvious risk of negative consequences.[39]

When assessing the ability to exercise the right to withdraw consent freely and at any time, attention must also be given to the specific characteristics of the process. „If you would not be able to fully action a withdrawal of consent – for example because deleting data would undermine the research and full anonymisation is not possible – then you should not use consent as your lawful basis (or condition for processing special category data). Consent is only valid if the individual is able to withdraw it at any time.) “[40].

3.6. Withdrawal of Consent in the Online Environment

In the online environment, in addition to issues related to obtaining consent, it is important that the possibility and the right to withdraw consent are taken into account and effectively implemented in practice.

[38] Ibid., Article 20.
[39] *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 13, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].
[40] *Information Commissioner's Office (ICO),* “What is Valid Consent?” <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> [27.11.2025].

For the full exercise of this right by the data subject, it is necessary that the digital environment and its specificities in practice comply with the requirements of the law. Establishing complex and multi-step procedures for withdrawing consent on a website directly indicates a lack of good faith on the part of the data controller and inconsistent respect for the rights of the data subject.

Consent should not be limited to a technical form or a mere click of a button — it must represent a genuine expression of will, based on the principles of transparency**,** being informed**,** and freely exercised choice**.**

4. International Practice and Challenges

The issue of considering consent as a legal basis for data processing, as well as its compliance with the law and the effective exercise of related rights, represents one of the current topics in international law. Analysis of practice shows that particular importance is attached to the principles of voluntariness**,** being informed**,** and transparency**.**

Furthermore, analyzing international practice provides an opportunity to assess the compliance of national legislation with international standards, to identify existing challenges, and to evaluate potential risks based on comparative analysis.

4.1. European Union (GDPR)

An important role in establishing international practice is played by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the General Data Protection Regulation (GDPR),[41] which defines the principles, rights, and obligations related to data processing, aimed at protecting the personal data of natural persons.

GDPR assigns particular importance to and clearly distinguishes the following mandatory characteristics of consent:

- Clear affirmative action
- Voluntariness
- Specificity
- Being informed
- Clarity[42]

In addition, GDPR provides for the burden of proof on the data controller**,** who must be able to demonstrate that consent was obtained for the data processing operation.[43] Furthermore, the regulation clearly highlights the risks arising when there

[41] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016
[42] Ibid., Recital 32.
[43] GDPR, Article 7(1).

is an apparent imbalance of power between the data controller and the data subject, particularly when the data controller is a public authority.[44]

Analysis of the consent-related provisions under GDPR reveals a clear similarity to the provisions of Georgian legislation and a comparable approach in regulatory practice. Specifically, in the examined cases, a uniform approach to expressing consent in a written document is observed, even when the document also regulates other matters. In discussions of the issue, it is clearly defined, in accordance with both national and international legislation, that the consent text/declaration must be separately distinguished from other matters and presented in a clear and easily understandable language**.**

There is also a direct correspondence between Georgian national legislation and GDPR provisions regarding the requirement to obtain consent. In both cases, the possibility to request consent freely and without limitation is considered a precondition for the correct formulation of consent and its implementation as a legally valid basis.[45]

International practice, particularly the provisions of GDPR, constitutes an important standard on which Georgian legislation and practice rely for guidance. International regulations demonstrate how the text requesting consent should be formulated to ensure the principles of voluntariness**,** being informed**,** and transparency**.**

Accordingly, GDPR serves not only as an educational and guidance instrument in the field of data protection, including in determining the lawfulness of processing operations, but also as a significant standard that supports the refinement of national legislation and the enhancement of current practice and legal awareness within society.

5. Conclusion

When considering the issue of consent as a legal basis for data processing, and evaluating the related statutory requirements and criteria, it becomes clear that what may initially appear as the simplest and most suitable basis for processing is, in fact, sufficiently complex and multifaceted. The associated protective mechanisms fully exclude the possibility of consent existing merely in a formal sense.

For the effective functioning of the consent institution, a combination of several factors is decisive — transparency**,** being informed**,** voluntariness**,** and the good faith of the data controller. When these criteria are collectively ensured, it can be concluded that the data subject's consent genuinely represents a free expression of will, rather than mere formality.

[44] Ibid., Recital 43.
[45] Ibid, Article 7(3).

The Information Commissioner's Office (ICO) establishes a general principle regarding the lawful basis of consent, according to which, whenever meeting the standard for consent is difficult, this is a sign that consent may not be an appropriate basis for data processing.[46]

In the contemporary digital environment, where the volume and frequency of data processing are unprecedented, particular importance is attached to the practical provision for obtaining and withdrawing consent — the user must be able to easily understand what they are consenting to and, if desired, withdraw it.

In the long term, it is essential that the consent institution does not become a formalistic mechanism, but rather serves as a real guarantee of the individual's awareness and freedom of choice. Establishing such an approach ensures the development of a data protection culture, effective application of legislation, and the strengthening of public trust in both the public and private sectors.

[46] *Information Commissioner's Office (ICO),* Guideline on *When is consent appropriate?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/

Bibliography:

1. Law of Georgia on Personal Data Protection 14/06/2023.
2. Guideline Recommendation of the Personal Data Protection Service of Georgia on "Obtaining Consent from the Data Subject," 10, 21.
3. Personal Data Protection Service of Georgia, "Guide for Individuals Interested in Creating a Website," 27.
4. EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).
5. UK General Data Protection Regulation (UK GDPR), <https://www.legislation.gov.uk/ukpga/2018/12/contents> [27.11.2025].
6. *The Autoriteit Persoonsgegevens (AP),* Legal Basis of Consent, <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-basics/legal-basis-of-consent> [27.11.2025].
7. *Cate, F. H.* The Failure of Fair Information Practice Principles In Consumer Protection in the Age of the Information Economy 2006, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972> [27.11.2025].
8. *CNIL (Commission nationale de l'informatique et des libertés),* Recommendation 5: Promote parental controls that respect the child's privacy and best interests, 09 August 2021, <https://www.cnil.fr/en/recommendation-5-promote-parental-controls-respect-childs-privacy-and-best-interests> [27.11.2025].
9. *Data Protection Commission (DPC),* Fundamentals for Child-Oriented Approach to Data Processing, December 2021, 29, <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf> [27.11.2025].
10. *European Data Protection Board (EDPB),* Guidelines on consent under Regulation 2016/679,2018, 7, <https://www.edpb.europa.eu/sites/default/files/files/file1/20180416_article29wpguidelinesonconsent_publish_en.pdf> [27.11.2025].
11. *EDPB,* Guidelines 05/2020 on consent under Regulation 2016/679, 10, 13, 19, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> [27.11.2025].
12. *Information Commissioner's Office (ICO),* Guideline on What is valid consent? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> [27.11.2025].
13. *Information Commissioner's Office (ICO),* Guideline on When is consent appropriate? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/> [27.11.2025].

14. *Swedish Authority for Privacy Protection*, The rights of children and young people on digital platforms, Stakeholder guide, 3, 15, 20, 40, <https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf> [27.11.2025].
15. European Court of Justice, CJEU, Case C-673/17, Planet49 GmbH [2019], §55, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143828> [27.11.2025].

Ginevra Cerrina Feroni[*]

Governing Artificial Intelligence through Data Protection: The Strategic Role of Independent Authorities in the Age of Algorithmic Power[**]

Artificial Intelligence (AI) represents not only a technological shift but also a constitutional challenge. As AI systems become more involved in social, economic and legal decisions, the role of Data Protection Authorities (DPAs) is becoming increasingly important. This short essay, based on the speech held by the Vice President of the Italian Data Protection Authority, Prof. Cerrina Feroni at the 33rd European Conference of Data Protection Authorities, examines the structural interdependence between AI and personal data, placing data protection at the core of AI governance. Drawing from the experience of the Italian DPA and comparative international examples, it analyses four critical areas: legal bases, data transfers, automated decision-making, and protection of vulnerable individuals, where DPAs are establishing the normative boundaries of AI systems. It further suggests that DPA's role might benefit from evolution from reactive enforcers to proactive institutional actors engaged in system design, audit, and risk classification. This essay tentatively suggests that the legitimacy, legal certainty, and democratic accountability of AI governance may be best served by the central involvement of independent supervisory authorities.

Keywords: Artificial Intelligence, Data Protection, Independent Authorities, GDPR, AI Governance, Algorithmic Accountability.

[*] Vice President of the Italian Data Protection Authority; Full Professor of Italian and Comparative Constitutional Law at the Faculty of Law of the University of Florence; Lawyer enrolled in the Special Register of University Professors; Member of the Board of the Italian Association of Comparative Public Law; Member of the Board of the Italian Association of Constitutionalists.

[**] The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

1. Introduction

It is fair to say that the field of Artificial Intelligence (AI) is having a significant impact on governance, institutional accountability, and fundamental rights protection. It is not a self-contained phenomenon, but rather a transformation that can be seen across public administration, private markets, and daily social interactions. It is interesting to note that a key distinguishing feature of AI, as opposed to previous technological advancements, is its capacity to make or influence decisions independently. Decisions that were once exclusively within the domain of human judgment and institutional procedures are now being influenced by AI. This reallocation of decision-making authority from humans to machines may entail a significant shift in how accountability, transparency, and rights are operationalised.

Moreover, the general-purpose nature of AI means that it has the potential to affect a wide range of regulatory domains, including consumer protection, labour law, media law, criminal justice and health governance. It is important to note that the way in which legal regimes intersect with one another can create zones of normative uncertainty, which has the potential to complicate the regulatory landscape. In such an environment, it may be that treating data protection as a sectoral concern is no longer sufficient. Otherwise, it shall be seen as a cross-sectional structural safeguard for democratic societies.

As AI evolves from a tool of optimization into an architecture of decision-making, it may be helpful to consider who should define its limits. It would be interesting to know who is responsible for ensuring its accountability and who is there to defend individuals when the effects of algorithmic systems on their lives are not always clear.

In the European legal tradition, it is understood that the defence of fundamental rights against technological overreach is best served by institutional rights-based mechanisms. Among these, Data Protection Authorities (DPAs) hold a unique position. They are equipped with investigative, corrective, and advisory powers, and are mandated to safeguard the rights enshrined in the Regulation (EU) 679/2016 (GDPR).

However, it is important to acknowledge that their role in the governance of AI systems is still evolving and, at times, contested. This essay aims to shed light on the importance of DPAs in shaping lawful, rights-compatible AI.

Drawing from practical enforcement experiences, legal doctrine, and comparative oversight practices, the following sections humbly suggest a proactive, interdisciplinary, and anticipatory model of data protection in the age of AI.

2. Artificial Intelligence and the Imperative of Data Protection

The relationship between AI and personal data is not incidental, but constitutive. It is fair to say that most advanced AI models, from generative systems to predictive analytics, are trained, refined, and deployed using data that describes or relates to individuals. No matter what form it takes, whether it be user prompts, sensor data or behavioural profiles, there are significant legal implications to consider.

Under the GDPR, personal data processing is permissible only under specific legal bases.[1] In the context of AI, particularly in the area of model training, consent and legitimate interest are often cited as the more relevant ones. However, it is important to acknowledge that both of these approaches have their challenges.

To be valid, consent must be informed, specific, freely given, and revocable. In opaque, large-scale training operations, meeting these criteria can sometimes be challenging.

On the other hand, legitimate interest requires a balancing test: this involves an assessment of whether the interests of the controller override the rights and freedoms of the data subject. In the field of AI, where risks can be intricate, cumulative, and challenging to anticipate, such evaluations necessitate a high degree of scrutiny.

Furthermore, cross-border data flows give rise to a number of additional challenges. It is important to note that AI developers often distribute computational tasks across jurisdictions, sometimes involving third countries without adequate legal safeguards. Even if Chapter V of the GDPR imposes strict conditions for such transfers, the process of enforcement can be hindered by a lack of transparency. Indeed, many developers may not disclose the location of data processing or storage, citing reasons such as trade secrets or technological complexity.

Finally, article 22 of the GDPR seeks to ensure that decisions made solely through automated processing do not have legal or similarly significant effects. Exceptions do exist, but they are subject to procedural guarantees, including the provision of meaningful information, the right to contest, and the involvement of human oversight.[2]

[1] See, in particular, articles 6 and 9 of the GDPR. While Article 6 outlines the general lawful bases for processing any personal data, Article 9 focuses specifically on the processing of special categories of personal data, which is more restricted.

[2] Article 22 of the GDPR states that:

"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

In this context, DPAs have begun to investigate and to initiate administrative proceedings that, in some cases, led to the imposition of fines. In Italy, the enforcement actions taken by the Italian Data Protection Authority (Garante) against Replika and ChatGPT have underscored the pressing need for urgent action, particularly in light of the absence of legal bases, the need for greater transparency, and the crucial importance of protecting minors. Similar interventions by Canada[3], South Korea[4], and Japan[5] confirm the global relevance of these concerns.

3. The Democratic Value of Independent Oversight

The governance of AI is not a neutral, technocratic exercise, but an area of contested power. AI systems influence behaviour, shape narratives, and generate knowledge and, moreover, have, in several cases, the potential to decide whether to guarantee or not the access to a range of services, including credit, employment, health, and public services. In this sense, the rules governing their operation and functioning are inherently political.

For this reason, DPA's role is not just about compliance. They are constitutional institutions with legal powers, technical competence and independence.

In this landscape, the institutional independence of DPAs is considered to be a democratic safeguard. Article 52 of the GDPR states that DPAs shall act with complete autonomy and independence, free from external influence. This independence should allow them to resist political and economic pressures, particularly in cases involving powerful multinational technology providers.

c) is based on the data subject's explicit consent

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. […]"

[3] On 4 April 2023, the Office of the Privacy Commissioner of Canada (OPC) announced an investigation into OpenAI. This followed a complaint regarding the collection and disclosure of personal data without consent. More information available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/.

[4] On 17 February 2025, South Korea's Personal Information Protection Commission (PIPC) announced that DeepSeek had suspended its app-based service in Korea in order to comply with the Personal Information Protection Act (PIPA). This followed an inquiry and technical evaluation by the PIPC, which revealed a lack of transparency in DeepSeek's privacy policy and un-notified third-party data transfers. More information available at:
https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2784#none.

[5] On 3 February 2025, Japan's Personal Information Protection Commission (PPC) published detailed information regarding Hangzhou DeepSeek Artificial Intelligence's privacy policy, shedding light on how the company collects, processes and protects user data. More information available at: https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/.

Experience has confirmed the value of this model. The Garante's investigation into ChatGPT[6], which led to a temporary restriction on processing, several corrective measures and a fine, was carried out independently, but in dialogue with European counterparts and civil society. It demonstrated that fundamental rights could be upheld even in cases that were moving quickly and receiving a lot of attention.

However, it shall be ensured that institutional independence is commensurate with institutional capacity. Effective oversight necessitates legal certainty, technical expertise and operational resources. In fact, DPA personnel must be equipped to not only respond to complaints, but also to conduct audits, interpret complex algorithmic systems, and engage in strategic foresight. Such institutional capacity, together with the independence requirement, aims to guarantee that DPAs are able to anticipate or intervene promptly on technological trends.

4. From Ex Post to Ex Ante: Redesigning the Supervisory Model

It is clear that the traditional regulatory model, based on ex post enforcement, is not always suitable when faced with the rapid pace, vast scale and intricate nature of AI. Intervening before harms occur is advisable, as this will render oversight more effective. A new supervisory paradigm shall be considered: a paradigm that combines ex post powers with ex ante engagement.

This change means that authorities need to take a more active role in designing and using AI systems. As a matter of example, tools such as regulatory sandboxes help DPAs and developers work together to identify and reduce risk in a controlled environment. Early dialogue has the potential to reduce uncertainty and promote compliance by design.[7]

It is also vital that DPAs contribute to the definition of risk classification systems. This is essential to ensure that data protection principles are embedded in the very architecture of AI regulation. Furthermore, DPAs shall have access to the technical underpinnings of AI whenever technically possible: documentation, training data and

[6] The Garante's investigation revealed several breaches of the GDPR carried out by OpenAI, with regard to the processing of user personal data. These violations included: failure to ensure transparency and to provide users with the necessary information, a failure to implement adequate age verification safeguards, a potential exposure of minors under 13 to inappropriate content, a failure to notify the relevant parties of a cybersecurity breach, and a disregard of an earlier order to conduct an urgent informational campaign. More information available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432.

[7] For this reason, since 2021, the Italian Data Protection Authority has been a permanent member of the FinTech Coordination Committee, which was established by the Ministry of Economy and Finance. The Committee oversees regulatory sandbox initiatives designed to test innovative financial solutions, including those based on AI and data-driven technologies. The sandbox initiative has received 53 applications since the launch of the first application window. 13 of them have been accepted. More information are available at: https://www.dt.mef.gov.it/it/attivita_istituzionali/sistema_bancario_finanziario/fintech/index_bak.html.

algorithmic logic, as operational transparency is, of course, an essential component of this process.

Without access to these layers, enforcement will not achieve its full potential.

In these sense, algorithmic audits, conducted by interdisciplinary teams, are a key tool. It is possible that these audits may reveal not only legal non-compliance but also structural risks such as bias, discrimination, or a lack of contestability. The integration of such practices within the framework of AI governance systems has the potential to enable the verification of compliance. The objective is not to impose excessive regulation, but rather to establish legal clarity. Responsible innovation becomes easier when expectations are known in advance. In order to ensure the efficacy of such enforcement and oversight mechanisms, they must be embedded within a broader, coordinated approach to AI governance.

5. Coordinated Governance and Rights-Based Convergence

AI governance involves many different stakeholders, such as regulators, competition and consumer authorities and, obviously, DPAs. This is due to the intricate nature of AI that produces effects on numerous areas. These may present challenges in terms of inconsistency, potential risks of fragmentation and jurisdictional conflict.

Hence, in the spirit of constructive dialogue, efforts shall be made to ensure an efficient coordination that is grounded in rights, with a view to avoiding outcomes that may be detrimental to all.

This process requires the presence of formal mechanisms of inter-institutional collaboration. As a matter of example, permanent coordination platforms, joint working groups and shared risk registers could be a way to align regulatory strategies. It is perhaps worth considering whether DPA members should have a more central role on these platforms, rather than playing a peripheral consultant role.

At the international level, convergence initiatives such as those of the Spring Conference of DPAs, G7, The OECD (Organisation for Economic Co-operation and Development), and Council of Europe offer promising frameworks, having the potential to contribute to the articulation of shared standards and supervisory priorities.

6. Conclusion

Artificial Intelligence is having an impact on the power relations between individuals, institutions and markets. It has the potential to influence the way in which decisions are made, information circulates, and rights are exercised or denied. In this context, governing AI might be interpreted as a means of governing power.

Data Protection Authorities have a unique role in ensuring that governance respects legality, proportionality, and accountability. They bring together legal authority, technical expertise, and institutional independence.

Their role is not to hinder innovation, but rather to guide it within the confines of democratic principles. For this reason, they are not only regulators, but also constitutional guardians of fundamental rights.

In order to achieve this potential, it is necessary for DPAs to be fully integrated into AI governance frameworks, to consider expanding their mandate from reactive enforcement to proactive engagement and to equip them with adequate resources and legal tools.

Bibliography:

1. Italian Data Protection Authority, Comunicato Stampa - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro, 2023. <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432>.
2. Ministero dell'Economia e delle Finanze. Sistema bancario finanziario <https://www.dt.mef.gov.it/it/attivita_istituzionali/sistema_bancario_finanziario/fintech/index_bak.htm>l.
3. Office of the Privacy Commissioner of Canada, OPC launches investigation into ChatGPT, 2023. <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/>.
4. Personal Information Protection Commission, Japan, Hangzhou DeepSeek Artificial Intelligence's privacy policy, 2025. <https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/>.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119.

Otar Chakhunashvili[*]

Salome Sigua[**]

Legal Aspects of Artificial Intelligence and Personal Data Protection Regulation: An Overview of National and International Practice[***]

The rapid development of information technologies and the integration of artificial intelligence (AI) into the public and private sectors have significantly expanded data processing activities. This process is accompanied by important legal and ethical challenges related to data protection.

The article aims to analyze the legal framework governing the processing of personal data by artificial intelligence systems in both international and national legislation. It examines the existing regulations, their effectiveness, and their compliance with the realities of modern technology.

Particular attention is given to the adequacy of current legal norms in addressing the unique capabilities and risks of AI, including issues of algorithmic bias, transparency, and the protection of users' rights.

Keywords: *Artificial Intelligence, personal data protection, algorithmic bias, protection of users' rights.*

1. Introduction

In the process of technological progress, numerous important issues arise, the fulfillment of which is considered essential in a democratic society. The protection of personal data is among those rights that have gained particular attention alongside the development of social relations and the means to regulate them. The right to

[*] Doctor of Law, Assistant Professor at the Faculty of Law of Ivane Javakhishvili Tbilisi State University. First Deputy Head of the Personal Data Protection Service.

[**] Invited Lecturer at the Faculty of Law of Ivane Javakhishvili Tbilisi State University.

[***] The article was prepared within the framework of the Young Scientists Grant Competition (YS-23-3460) funded by the Shota Rustaveli National Science Foundation of Georgia.

personal data protection is generally viewed as part of the broader right to privacy or the right to respect for private life. At first glance, these two rights may appear analogous and even interchangeable. However, within the European context, both are regarded as vital components of a sustainable democracy.

It is undeniable that artificial intelligence represents one of the latest scientific achievements in humanity's technological development, which will be applied — and indeed dominate — many fields in the near future. The Fourth Industrial Revolution can essentially be characterized by the development of new technologies such as artificial intelligence, robotics, nanotechnology, quantum computing, biotechnology, the Internet of Things (IoT), and blockchain, all of which will transform the way society lives and works.

There are many questions surrounding artificial intelligence; however, one of the most pressing issues today concerns the processing of personal data by AI systems. This technology is rapidly evolving, and the data it processes vary in both volume and content. Artificial intelligence learns from information obtained from multiple sources and processes vast amounts of data based on pre-defined algorithms. Consequently, it can be said that data have become the only "fuel" for artificial intelligence.

2. Analysis of National and International Legislative Acts Regulating Personal Data

Personal data refer to any information relating to an identified or identifiable natural person. Personal data may also consist of a combination of different pieces of information that, when processed together, allow the identification of an individual.[1] According to the legislation of the European Union and the Council of Europe, personal data are defined as information relating to an identified or identifiable natural person[2] whose identity is known or can be determined based on additional information. In determining whether a person is identifiable, the controller or any other entity engaged in data processing must take into account all reasonable means that could be used, either directly or indirectly, to identify the individual.[3]

The principle of the rule of law is one of the most important foundations of a democratic state.[4] In a state governed by the rule of law, the highest social values are

[1] European Commission, What is personal data? <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> [17.01.2024].
[2] General Data Protection Regulation, Article 4(1); Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+"), Article 2(a).
[3] General Data Protection Regulation, Recital 26.
[4] Decision of the Constitutional Court of Georgia of 27 March 2017, No. 1/4/757, in the case "Citizen of Georgia Giorgi Kraveishvili v. Government of Georgia", Section II-4.

recognized as the individual, their dignity, rights, and freedoms. Accordingly, the state exists to serve its people, who themselves are the source of state authority.[5]

As most social and economic activities are now conducted online, greater importance has been attached to the protection of personal data and the right to privacy. According to recent data, out of 194 countries worldwide, 137 countries have adopted legislative acts regulating personal data protection, accounting for 71% of all states. It is noteworthy that 9% (approximately 17 countries) are in the process of developing such legislation, 15% (around 30 countries) have not yet adopted any, and for 5% (around 9 countries) no information is available.[6] It is significant that the majority of countries without personal data protection legislation are located on the African continent, while the countries for which information is unavailable are found both in Africa and Indonesia.

The adoption of international legal instruments related to personal data protection began in the 1970s,[7] when information technologies came into intensive use and several countries introduced legislation to regulate the processing of personal information by public authorities and large corporations. As a result, various data protection mechanisms[8] were established across Europe, and over time, data protection evolved into an independent value, no longer viewed merely as part of the right to privacy. Within the European Union's legal system, data protection is recognized as a fundamental right, distinct from the right to respect for private life.

The United Nations legal framework does not explicitly recognize personal data protection as a fundamental right, even though the right to privacy has long been acknowledged as such under international law. Specifically, Article 12 of the Universal Declaration of Human Rights (UDHR) concerns the right to respect for private and family life.[9] This declaration was the first international instrument to affirm that every person has the right to protect their private sphere from interference by others, particularly by the state. Although the UDHR does not have binding legal force, it holds significant status as the foundational instrument of international human rights law and has strongly influenced the development of human rights mechanisms in Europe. The Declaration distinguishes the inviolability of private life from unlawful interference not only by state authorities but also by private individuals (such as neighbors, employers, etc.).[10]

In addition to the Universal Declaration of Human Rights, various international instruments adopted by the United Nations have established global standards for the

[5] Scientific Journal "Young Lawyers", No. 5, joint publication of "Young Lawyers" and the "Educational Center of Lawyers", Tbilisi, 2016, 34.

[6] UN Trade&Development, Data Protection and Privacy Legislation, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> [17.01.2024].

[7] Handbook on European Data Protection Law, Publications Office of the European Union, 2018, 22.

[8] The European Union developed its first comprehensive data protection instrument in 1995: Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[9] Universal Declaration of Human Rights, Article 12.

[10] *Alfredsson G., Eide Asbjorn,* The Universal Declaration of Human Rights A Common Standard of Achievement, Hague, Kluwer Law International, 1999, 257-258.

protection of privacy and private life. The first such instrument following the Declaration was the International Covenant on Civil and Political Rights (ICCPR), which entered into force in 1976. The ICCPR affirms that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[11] As an international treaty, it obliges signatory states to respect and protect civil rights, including the right to privacy. In 1989, the UN General Assembly adopted the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, which prohibits arbitrary or unlawful interference with the privacy, home, family, correspondence, or other rights of migrant workers and their family members. Subsequently, in 2006, the Convention on the Rights of Persons with Disabilities further defined the right to privacy and confidentiality for persons with disabilities, establishing binding obligations for its signatory states.

Soon after the adoption of the Universal Declaration of Human Rights, the right to respect for private life was also recognized in Europe. In 1950, the European Convention on Human Rights (ECHR) was adopted, establishing the fundamental right to respect for private life.[12] According to Article 8 of the ECHR, everyone has the right to respect for their private and family life, home, and correspondence. No public authority may interfere with the exercise of this right except as provided by law and when such interference is necessary in a democratic society for legitimate and significant public interests.

The adoption of international legal instruments concerning the protection of personal data mainly began between the 1960s and 1980s. With the emergence of information technologies in the 1960s, there arose an increasing need for detailed rules governing the protection of personal data. By the mid-1970s, the Committee of Ministers of the Council of Europe had adopted several resolutions on personal data protection, referring explicitly to Article 8 of the European Convention on Human Rights.[13] The first international instrument dedicated to the protection of personal data was the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[14], also known as Convention No. 108. Adopted in 1981, it was ratified by the Parliament of Georgia in 2005.[15] This Convention was, and remains, the only international treaty with binding legal force in the field of data protection. It safeguards an individual's right to know what

[11] International Covenant on Civil and Political Rights (ICCPR), 1976, Article 17.

[12] European Convention on Human Rights, 1950, Article 8.

[13] Council of Europe, Committee of Ministers (1973), Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, 26 September 1973; Council of Europe, Committee of Ministers (1974), Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, 20 September 1974.

[14] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.

[15] EU Treaty Office, <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108> [20.01.2024].

information is held about them and, where necessary, to request its correction. Restrictions on the rights provided under the Convention are allowed only in cases involving overriding interests, such as national security or defence. Furthermore, the Convention provides for the free flow of personal data between the contracting parties while imposing certain restrictions on transfers to states whose legal frameworks do not ensure an adequate level of data protection.

In 2001, an Additional Protocol to Convention 108 was adopted, introducing provisions on international data transfers to states that are not Parties to the Convention (so-called "third countries"), as well as a mandatory requirement for the establishment of a data protection supervisory authority at the national level. Most importantly, the Additional Protocol expanded the scope of the Convention.[16]

From 1995 until May 2018, the principal legal instrument for data protection within the European Union was Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (commonly referred to as the Data Protection Directive).[17] Adopted in 1995, the Directive aimed to harmonise the data protection laws of EU Member States, many of which already had national legislation in place, in order to ensure a high and consistent level of personal data protection and to facilitate the free flow of data between Member States. The free movement of goods, capital, services, and people within the internal market also required the unrestricted movement of data—something that could not be achieved without establishing an equally high standard of data protection across all Member States.

The General Data Protection Regulation (GDPR) was adopted by the European Union in 2016 to replace the previous directive adopted in 1995, at a time when the Internet was still in its infancy. The earlier directive proved insufficient to address the challenges posed by modern technologies and the digital environment, making it necessary to reform and replace it with a new, more comprehensive legal framework.[18] The GDPR has direct legal force across all EU Member States, although each state has updated its national data protection legislation to ensure full compliance with it.

The Constitution of Georgia guarantees individuals the right to respect for their private and family life, privacy of communication, and informational self-determination. It also stipulates that information contained in official records relating to a person's health, finances, or other personal matters shall not be accessible to others without that person's consent, except in cases provided by law where such

[16] Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, CETS No. 181, 2001.

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

[18] EDPS, The History of the General Data Protection Regulation, <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> [15.01.2024].

access is necessary to ensure state or public security, protect public interests, public health, or the rights of others. This provision serves as the constitutional foundation for personal data protection in Georgia, the guarantees for which are implemented through various legislative acts, including the Law of Georgia "On Personal Data Protection."

The Law of Georgia "On Personal Data Protection" is the core legislative act governing the field of personal data protection. Its initial version entered into force on November 1, 2014, and was subsequently amended several times to bring it closer to international standards.

With the adoption of the new Law of Georgia "On Personal Data Protection," national legislation in this field has been substantially harmonized with European standards, thereby ensuring the introduction of internationally recognized principles and best practices in data protection. Following the adoption of the EU General Data Protection Regulation and the modernization of Convention 108, further alignment with European standards became necessary. Consequently, in 2023, the Parliament of Georgia adopted the new Law "On Personal Data Protection," which entered into force on March 1, 2024.[19]

Among the innovations introduced by the new law are the obligations imposed on controllers to manage risks arising from technological progress, particularly through the implementation of data protection impact assessments and the incorporation of the principles of "Privacy by Design" and "Privacy by Default." These provisions represent significant advancements in Georgian data protection law, aiming to proactively identify and mitigate potential risks to human rights in the context of rapid technological development.

Currently, the Law of Georgia "On Personal Data Protection" serves as the principal legislative framework regulating the fundamental principles of data processing and the legal aspects of automated data processing, including the use of AI systems. Under the law, data processing must pursue a legitimate purpose, adhere to the principle of protection against unlawful interference, and safeguard the rights of data subjects, including their rights to information, access, rectification, erasure, and objection.

3. Analysis of National and International Acts Regulating Artificial Intelligence

There is no doubt that artificial intelligence is one of the most important and most modern scientific achievements of technological progress, destined to significantly transform many fields in the near future and become firmly established within them. The fourth industrial revolution is closely linked to the development of innovative technologies — including artificial intelligence, robotics, nanotechnologies, quantum

[19] Law of Georgia on Personal Data Protection, 14/06/2023.

computing, biotechnology, the Internet of Things (IoT) and blockchain — technologies that will substantially reshape both our daily lives and patterns of work and activity.[20]

Artificial intelligence (AI) denotes the intelligence of computer machines that act as "intelligent agents." The term is used when a computer system seeks to imitate cognitive functions.[21]

The principal problems for personal data protection arise, on the one hand, from the volume and broad variety of personal data being processed, and on the other hand from the processing methods and their outcomes. The deployment of complex algorithms and software to transform large datasets into decision-making resources affects various groups of data subjects, in particular through profiling and discriminatory practices, and ultimately gives rise to serious data-protection concerns.[22]

Regulating artificial intelligence is a complex global challenge because it raises ethical, legal and technical issues. Given the rapid pace of AI development, legal regulation remains difficult for many states; as a result, regulation has largely taken the form of policy documents and national strategies. The mere adoption of action plans or framework documents is not a panacea, as demonstrated by the limited practicality of some country-level documents. The term "strategy" is widely used in contemporary political science and management, yet no single agreed definition exists; strategy is often understood primarily as a written strategic plan.

Canada adopted the first national AI strategy in 2017, soon followed by Japan and China; in the same year, Singapore and Finland also approved AI strategies. Since 2018, momentum has accelerated: the United States, Taiwan, Italy, the United Kingdom, Sweden, Mexico, Denmark, France, Australia, South Korea, Germany and India[23] adopted similar strategies, and the European Union approved its own AI development strategy in 2018.

On 13 March 2024, the European Parliament voted in plenary to support the European Commission's proposal for a regulation establishing harmonised rules on artificial intelligence (the "AI Act") (523 in favour; 46 against; 49 abstentions).[24] The AI Act is a binding instrument for EU Member States that aims to regulate the design, development and use of AI systems. It applies across the Union to both the public and private sectors, with specified exceptions — notably for AI systems intended for military, defence, national security, and certain research and development purposes. The Act imposes different obligations according to the potential risks and impacts of

[20] *Gabisonia, Z.,* Internet Law and Artificial Intelligence, "World of Lawyers," Tbilisi, 2022, 513.

[21] *Stuart Russel and Peter Norvig*, Artificial Intelligence: A Modern Approach (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, 27, 32–58, 968–972; *Stuart Russel and Peter Norvig*, Artificial Intelligence: A Modern Approach (3rd ed.), 2009, Upper Saddle River, New Jersey: Prentice Hall, 2.

[22] Council of Europe, Consultative Committee of Convention 108, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 2.

[23] *Dutton T.,* An Overview of National AI Strategies, Politics + AI 2018, <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> [10.03.2024].

[24] OneTrust DataGuidence, <https://www.dataguidance.com/news/eueuropean-parliament-adopts-ai-act> [12.03.2024].

AI systems, classifying them into three main categories — "unacceptable risk," "high risk," and "limited risk" — with corresponding requirements for each category.

The Council of Europe Framework Convention on Artificial Intelligence, aimed at protecting human rights, democracy and the rule of law, is among the first international legal instruments to set standards for the development and use of AI that fully respect human dignity, personal freedoms and equality. The Convention emphasises that technological progress must not undermine human rights or democratic values. It prioritises transparency, accountability and security—essential conditions for creating systems that respect individual autonomy and safeguard data protection. Both the State and the private sector are required to take appropriate measures to prevent harm and to ensure effective protection of human rights, including through risk assessment, oversight and compensation mechanisms. The Convention's approach opposes discrimination and promotes fair and responsible use, thereby fostering not only technological development but also public trust and the preservation of the foundations of democratic governance.

The Organization for Economic Co-operation and Development (OECD) adopted its first Recommendation on Artificial Intelligence in 2019 to promote innovation while strengthening trust in AI systems and safeguarding fundamental human rights and freedoms. In 2023 the Recommendation was updated to provide a clearer definition of an artificial intelligence system in response to rapid technological developments. The OECD Recommendation sets out five high-level, value-based principles and five recommendations for national policy and international cooperation. However, these Recommendations are non-binding.[25]

In the United States, the White House Office of Science and Technology Policy published a non-binding plan on October 4, 2022, containing five principles designed to minimise harm from automated systems. On August 18, 2022, the National Institute of Standards and Technology (NIST) released the second draft of the AI Risk Management Framework, intended to help organisations that develop or deploy AI assess and manage associated risks. The Framework consists of voluntary guidelines and recommendations and is therefore non-binding.[26]

China[27] adopted its "Next-Generation Artificial Intelligence Development Plan" in 2017 and published Ethical Guidelines for the Governance of Artificial Intelligence in 2021. In January 2022, China introduced two laws addressing specific AI applications. The Algorithm Provisions for the Governance of Algorithmic Recommendations for Internet Information Services came into force in March 2023, while the Draft Deep

[25] OECD Recommendation of the Council on Artificial Intelligence, 2024

[26] *Kohn B., Pieper F. U.,* AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[27] *Klimentov M.,* From China to Brazil, here's how AI regulated around the world, September 2023, <https://www.washingtonpost.com/world/2023/09/03/ai-regulation-law-china-israel-eu/?trk=article-ssr-frontendpulse_little-text-block> [25.03.202].

Synthesis Provisions for the Governance of Internet Information Services remain at the draft stage.

Japan[28] has the second-largest IT sector among OECD countries and is heavily invested in research and development. It was also the second country to develop a national AI strategy. The "AI Technology Strategy," published in March 2017, includes an industrialization roadmap for AI services and structures AI development into three phases: Processing data for AI; 2. Public use of AI; and 3. Creation of AI ecosystems.

Japan's AI strategies and regulations are closely aligned with the country's broader "Society 5.0" initiative. The "Social Principles for Human-Centered Artificial Intelligence," developed by the Integrated Innovation Strategy Promotion Council and published by the Japanese government in March 2019, set out fundamental principles to guide the development of an AI-enabled society. The document outlines seven key social principles that society and the state should uphold in their approach to AI: (1) human-centeredness, (2) education and literacy, (3) data protection, (4) security, (5) fair competition, (6) fairness, accountability and transparency, and (7) innovation. These principles, however, are non-binding and serve primarily as policy guidance.

Brazil[29] is currently in the process of developing legislation to regulate AI. On December 1, 2022, the Brazilian Senate's Non-Permanent Jurisprudence Committee presented a report on AI regulation, which included a draft law. According to the committee's rapporteur, the proposed regulation is based on three central pillars: (1) safeguarding the rights of individuals affected by AI systems, (2) classifying levels of risk, and (3) establishing governance measures for companies that develop or operate AI systems.

The draft law also grants data subjects the right to request and obtain information from AI system providers regarding the scope and purpose of personal data processing.

Canada[30] was among the first countries to adopt a national AI strategy. In 2017, it introduced the five-year "Pan-Canadian AI Strategy," focused on fostering AI research and talent development. Unlike the strategies of many other countries, Canada's approach primarily emphasizes research, innovation, and the accumulation of knowledge in the field.

On June 16, 2022, the Canadian federal government introduced Bill C-27, known as the Digital Charter Implementation Act, which includes the Artificial Intelligence and Data Act (AIDA). AIDA regulates interprovincial and international trade in AI systems and seeks to mitigate risks and biased outcomes associated with high-impact AI

[28] *Habuka H.*, Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency, Report 2023, <https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7 presidency#:~:text=As%20mentioned%20above%2C%20there%20are,occurs%20due%20to%20AI%20systems?trk=article-ssr-frontend-pulse_little-text-block> [30.03.2024].

[29] *Kohn B., Pieper F. U.,* AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[30] *Gabisonia, Z.,* Internet Law and Artificial Intelligence, "World of Lawyers," Tbilisi, 2022, 526.

technologies. The law also empowers the government to restrict the use of AI systems that significantly infringe upon the legitimate rights and interests of individuals.[31]

Switzerland[32], in contrast to the European Union, does not consider it necessary to adopt a dedicated law regulating artificial intelligence. The Swiss government maintains that existing legal frameworks can be adapted to address AI-related challenges. For instance, the Data Protection Act contains provisions on AI transparency, while competition law, product liability law, and the Civil Code have been updated with relevant rules governing the use of artificial intelligence.

The UK[33] government began publishing sectoral reports on artificial intelligence in 2018 as part of its broader Industrial Strategy. Subsequently, on 29 March 2023, it released an AI White Paper outlining proposals for regulating the use of artificial intelligence (AI) in the UK. This document builds on the earlier AI Regulation Policy Paper, which articulated the government's vision for a "pro-innovation" and "context-specific" AI regulatory regime.

The UK approach diverges from the model adopted in the EU AI Act, as it does not introduce new, comprehensive legislation. Instead, it focuses on establishing principles and expectations for the development and deployment of AI, while empowering existing regulatory bodies—such as the Information Commissioner's Office (ICO), the Financial Conduct Authority (FCA), and the Competition and Markets Authority (CMA)—to issue guidance and oversee AI applications within their respective mandates.

Denmark's[34] strategy, titled "Denmark's Digital Growth" (2018), aims to position the country as a global leader in the digital industrial revolution, thereby fostering national prosperity and economic growth.

Germany[35] also adopted a national Artificial Intelligence Strategy in 2018, jointly developed by the Federal Ministries of Economic Affairs, Research, and Labour. The German government seeks to safeguard its position as a leading research hub, enhance industrial competitiveness, and promote the application of AI across all sectors of society. To achieve these objectives, it committed an additional €500 million in 2019 to further AI policy initiatives.

---

[31] Government of Canada, The Artificial Intelligence and Data Act (AIDA)- Companion document, <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document?trk=article-ssr-frontend-pulse_little-text-block> [01.04.2024].

[32] *Kohn B., Pieper F.U.,* AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].

[33] *Prinsley M.A., Yaros O., Randall R., Hajda O., Hepworth E.,* UK's Approach to Regulating the Use of Artificial Intelligence, <https://www.mayerbrown.com/en/insights/publications/2023/07/uks-approach-to-regulating-the-use-of-artificial-intelligence> [10.04.2024].

[34] Agency for Digital Government, The Danish National Strategy for Artificial Intelligence, <https://en.digst.dk/strategy/the-danish-national-strategy-for-artificial-intelligence/> [10.04.2024].

[35] German Federal Government's AI Strategy, <https://www.bmwk.de/Redaktion/EN/Artikel/Technology/artificial-intelligence.html> [12.04.2024].

India's[36] National Strategy for Artificial Intelligence (2018) emphasizes the use of AI not only as a driver of economic growth but also as a tool for social inclusion. Recognizing its position as one of the world's fastest-growing economies, India aims to leverage AI for transformative, inclusive, and sustainable development aligned with its broader socio-economic goals.

Italy[37] published an AI White Paper in 2018, which, unlike many other national strategies focused primarily on research or private sector adoption, concentrates on promoting the integration of AI technologies within public administration and improving government efficiency.

Malaysia[38] adopted its Artificial Intelligence Strategy 2021–2025 (AI-Rmap) in 2021, setting out a national roadmap for developing AI capabilities over a five-year period. The COVID-19 pandemic served as a catalyst for accelerating digital transformation, shaping Malaysia's strategic vision for AI. AI-Rmap was developed with three distinctive features: (1) alignment with global and national strategies on science, technology, and innovation; (2) a collaborative "Quadruple Helix" approach involving government, academia, industry, and society (GAIS); and (3) an entirely virtual development process, from inception to completion. The overarching goal is to establish a robust and sustainable AI innovation ecosystem, transforming Malaysia into a high-income, technologically advanced nation through the strategic application of artificial intelligence.

The Polish[39] government initiated discussions on the development of a national artificial intelligence strategy in May 2018 by convening the first roundtable dedicated to this topic. Subsequently, in December 2020, the Council of Ministers adopted the Polish National AI Strategy. The document encompasses a broad range of policy areas, including society, education, science, business, public administration, and international cooperation. It emphasizes the protection of human rights and dignity, the promotion of fair competition, and the establishment of an ethical framework for trustworthy AI. Furthermore, Poland aims to create conditions that foster the growth of an AI ecosystem across ethical, legal, technical-operational, and international dimensions.

Singapore[40] launched a five-year National AI Programme in 2017, supported by an investment of USD 150 million to enhance national capabilities in the field of artificial intelligence. Building on these efforts, in 2019 Singapore introduced its first National AI Strategy (NAIS), outlining measures to integrate AI into key sectors to drive

[36] India's National Strategy for Artificial Intelligence, 2018, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> [17.04.2024].

[37] European Commission, National strategies on Artificial Intelligence, A European perspective in 2019, Country report – Italy, <https://knowledge4policy.ec.europa.eu/sites/default/files/italy-ai-strategy-report.pdf> [17.04.2024].

[38] Navigating the Future Malaysia's Ethical AI Vision, <https://thesun.my/business/navigating-the-future-malaysia-s-ethical-ai-vision-IP12485793> [29.05.2024].

[39] Poland AI Strategy Report, <https://ai-watch.ec.europa.eu/countries/poland/poland-ai-strategy-report_en> [18.04.2024].

[40] National Artificial Intelligence Strategy 2.0 to Uplift Singapore's Social and Economic Potential, 2023, <https://www.smartnation.gov.sg/media-hub/press-releases/04122023/> [15.04.2024].

economic transformation. The government's updated NAIS 2.0 demonstrates Singapore's continued ambition to build a trusted, human-centric, and responsible AI ecosystem. The revised strategy focuses on fostering innovation, promoting public and private engagement, and ensuring that AI contributes to sustainable economic growth. Recognizing both the opportunities and challenges presented by AI, Singapore underscores the importance of responsible governance and risk mitigation to harness AI's potential while preventing adverse social and ethical consequences.

The Republic of Korea[41] adopted its National AI Strategy on 17 December 2019, under the vision "Towards a World Leader in AI Beyond IT." The strategy seeks to enhance Korea's digital competitiveness, generate significant economic value from AI technologies, and improve quality of life by 2030.

Sweden's[42] National AI Strategy, published in May 2018, outlines the government's overall policy direction for artificial intelligence. The strategy aims to establish a foundation for future initiatives to advance Sweden's prosperity and competitiveness through AI. It identifies four priority areas—education, research, innovation, and infrastructure—as key drivers of national development in this field.

The United Arab Emirates (UAE)[43] launched its Artificial Intelligence Strategy in 2017, positioning itself as a pioneer in the Middle East and becoming the first country globally to establish a dedicated Ministry[44] of Artificial Intelligence.[45] The central objective of the UAE's AI Strategy is to enhance government efficiency through the adoption of artificial intelligence technologies. Moreover, the UAE's long-term vision aims to position the country as a global leader in AI by 2031, reflecting its commitment to digital transformation and innovation-led governance.

In May 2018,[46] the ministries responsible for digital development in Denmark, Estonia, Finland, the Faroe Islands, Iceland, Latvia, Lithuania, Norway, Sweden, and the Faroe Islands published a Declaration on Artificial Intelligence in the Nordic–Baltic Region. The participating countries agreed to cooperate in order to *"develop and promote the use of artificial intelligence for the benefit of people."* The declaration identified seven key areas of cooperation: 1. improving opportunities for skills

[41] National Strategy for Artificial Intelligence of Korea, <https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10&mPid=9> [15.04.2024].

[42] European Commission, National Strategies on Artificial Intelligence. A European perspective in 2019, Country report Sweden, <https://knowledge4policy.ec.europa.eu/sites/default/files/sweden-ai-strategy-report.pdf> [15.04.2024].

[43] UAE National Strategy for Artificial Intelligence 2031, <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf> [15.04.2024].

[44] Ministry of Artificial Intelligence of the United Arab Emirates, <https://ai.gov.ae/> [15.04.2024].

[45] UAE Strategy for Artificial Intelligence, <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-strategy-for-artificial-intelligence> [15.04.2024].

[46] Nordic Co-operation, AI in the Nordic-Baltic region, <https://www.norden.org/en/declaration/ai-nordic-baltic-region> [17.04.2024].

development; 2. increasing access to data; 3. developing ethical and transparent guidelines, standards, principles, and values; 4. establishing standards for hardware and software that ensure privacy, security, and trust; 5. ensuring that artificial intelligence plays a significant role in European discussions on the Digital Single Market; 6. avoiding unnecessary regulations; and 7. utilizing the Nordic policy framework of the Nordic Council of Ministers to facilitate regional collaboration.

As for Georgia, it is noteworthy that since 2024 the country has signed the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. As a post-Soviet state that is still in the process of developing its high-tech sector,[47] Georgia faces particular challenges in the creation and regulation of artificial intelligence systems. According to a 2024 statement by the Minister of Justice, technological progress necessitates the introduction of legal regulations that both promote innovation and safeguard human rights. To this end, an interdepartmental working group is being established within the Ministry of Justice to develop a legal framework for the regulation of AI compatible with EU law.

At present, there is no specific legislative act in Georgia that directly regulates the legal status, scope, or ethical standards applicable to artificial intelligence. While the use of technology is governed by general legal norms—such as the constitutional guarantee of privacy, the Law of Georgia on Personal Data Protection, and other sectoral acts—there are no explicit provisions addressing:

- Criteria for algorithmic transparency;
- The legal assessment of decision-making automation; or
- Ethical frameworks for the use of AI in the public and private sectors.

The Law of Georgia on Personal Data Protection does not contain explicit rules on AI but includes provisions relevant to automated data processing, which may encompass certain AI applications. Under the law, automated decision-making is permitted only if the accuracy, awareness, security, and rights of the data subject are ensured. Nevertheless, the law does not yet reflect the specific risks and regulatory challenges posed by AI technologies, highlighting the need for an additional legislative framework tailored to contemporary developments.

It is also important to note that in 2025, the Georgian government approved the Georgian Digital Governance Strategy 2025–2030, which proactively incorporates the development of an ethical and legal framework for the governance and regulation of artificial intelligence.[48]

The examples discussed above do not represent an exhaustive global picture. A growing number of countries are developing policy frameworks and action plans in this area. For instance, Argentina, Chile, Colombia, and Israel have adopted policy documents addressing artificial intelligence, while Australia, Bangladesh, Egypt, Indonesia, Mauritius, Peru, and Saudi Arabia have implemented national AI action plans. In Taiwan, the government is actively working on the adoption of a legislative

[47] Announcement available at: https://justice.gov.ge/?m=articles&id=OrginiwJBU

[48] Decree No. 100 of the Government of Georgia of April 3, 2025, On the Approval of the "Digital Governance Strategy of Georgia 2025–2030" and the "Action Plan for 2025–2026 of the Digital Governance Strategy of Georgia 2025–2030."

act on artificial intelligence; a draft law has already been prepared and is currently awaiting approval.

4. The Relationship Between Artificial Intelligence and Personal Data at the Legislative Level

Artificial intelligence has long ceased to be merely a technology of the future; in many respects, it has become a product of the present—one that, alongside simplifying everyday life, also poses numerous challenges for both developers and users. One of the most significant challenges concerns the boundary between the benefits of artificial intelligence and the protection of personal data. As the scope of artificial intelligence expands, so too do the risks associated with personal data. A clear example of this can be found in social networks, which are becoming increasingly enriched with automated, intelligent algorithms each year. Altogether, this enables AI-based systems to monitor our online activities, which in effect constitutes interference with our private lives.[49]

In the process of data processing carried out by artificial intelligence, the core principles of the General Data Protection Regulation (GDPR)—such as accountability, transparency, lawfulness, and data minimization—are often violated. AI systems frequently collect data in ways that do not clearly specify the purposes for which it will be used, thereby contradicting the principle of purpose limitation. Moreover, data is often processed without a valid legal basis, stored for indefinite periods, and used for purposes not previously agreed upon, thereby infringing the requirement of data minimization. Given the complexity and rapid development of technology, ensuring effective control and audit mechanisms proves difficult, which poses an additional challenge from the perspective of data protection.[50]

Artificial intelligence (AI) possesses the capability to recognize patterns that are imperceptible to the human eye, to learn, and to make predictions concerning individuals and groups. In this sense, AI can generate information that is otherwise difficult to obtain or may no longer exist. Consequently, data collected and processed through AI technologies can be used for longer periods and for broader purposes than those for which it was originally and consciously disclosed. The enhanced analytical and predictive capacities of AI are therefore likely to create an environment in which an individual can be identifiable based on information generated by, or associated with, them.[51]

[49] Council of Europe, Consultative Committee of Convention 108, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 2.

[50] *Chalubinska-Jentiewicz K., Nowikowska M.,* Artificial Intelligence v. Personal Data, Polish Political Science Yearbook, vol 5., Poland 2022, 188-189.

[51] OVIC, Artificial Intelligence and Privacy – Issues and Challenges, <https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/> [05.05.2024].

AI systems enable the use of personal data of all categories for the purposes of analysis, prediction, and behavioral influence. Artificial intelligence transforms this data, and the results derived from it, into valuable products. In particular, AI makes possible the automation of decision-making processes in domains that traditionally require complex human judgments based on multiple and sometimes undefined criteria. In many instances, automated predictions and decisions can be not only more efficient but also more accurate and impartial than those made by humans, as AI systems are capable of avoiding typical cognitive biases and can be subjected to systematic oversight. However, algorithmic decisions are not immune to error or discrimination, and their misuse can result in violations of individual rights and freedoms.[52] It is noteworthy that under the Law of Georgia on Personal Data Protection, a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects concerning them.[53] As already noted, automated means may include artificial intelligence systems.

Since no specific legislative acts regulating artificial intelligence have yet been adopted, the relationship between artificial intelligence and personal data remains undefined at the legislative level. Nevertheless, it may be inferred that the personal data protection laws of most countries contain a general provision stating that data processing may be carried out by both automated and non-automated means—a formulation broad enough to be interpreted as encompassing the use of artificial intelligence systems.

At the international level, the European Union's Artificial Intelligence Act represents the first comprehensive legal framework establishing binding standards for the development, deployment, and use of AI systems, including obligations concerning the protection of personal data and privacy. Articles 7 and 8 of the Act explicitly guarantee the inviolability of private life and the respect for personal data, linking AI governance directly to fundamental rights protection.[54] Similarly, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law constitutes the first-ever legally binding international treaty in this domain, and it is of particular relevance for Georgia as a signatory state.

Pursuant to Article 28 of the EU AI Act, when artificial intelligence is used in the field of healthcare, the fundamental rights protected under the Charter of Fundamental Rights of the European Union—including the rights to private and family life and to personal data protection—must be fully respected. The Act also emphasizes that AI systems applied in the areas of migration, asylum, and border control affect individuals who are often in particularly vulnerable positions and dependent on the decisions of state authorities. Therefore, ensuring the accuracy, transparency, and

[52] European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020,
<https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [05.05.2024].

[53] Law of Georgia on Personal Data Protection, Article 19.

[54] European Union Artificial Intelligence Act (EU AI Act), Paragraph 2.

non-discriminatory operation of AI systems in these contexts is essential for safeguarding the fundamental rights of the affected individuals.[55]

The Peruvian executive adopted a law promoting the use of artificial intelligence for economic and social development, introducing a risk-based regulatory approach similar to that of the European Union's AI Act. The law classifies potential risks, restricts certain high-risk systems, and explicitly incorporates data protection and privacy principles.[56] One of its core provisions refers to the principle of "privacy in artificial intelligence," according to which AI systems must not infringe upon individuals' privacy.[57] The right to privacy, understood broadly, encompasses the protection of private life, communications, and personal space from external interference. The right to personal data protection, while closely related, is a distinct aspect of this right, focusing specifically on ensuring that personal data are collected, processed, and stored lawfully, fairly, and transparently.

An interesting aspect of Saudi Arabia's strategy is that, since its establishment, the Saudi Data and Artificial Intelligence Authority (SDAIA) has been leading the national data and artificial intelligence agenda to advance the objectives of the Kingdom's Vision 2030. Most recently, SDAIA, in partnership with the Ministry of Communications and Information Technology (MCIT), has chaired the G20 Digital Economy Working Group and spearheaded the Kingdom's response to Covid-19 through the launch of applications such as Tawakkalna and Tabaud. In addition, the government has issued a series of policies – including the Kingdom's Data Classification Policy, Personal Data Protection Policy, Data Sharing Policy, Freedom of Information Policy, and Open Data Policy – thereby paving the way for a robust and business-friendly regulatory environment.

Below are several court decisions addressing the intersection between artificial intelligence and personal data.

On June 28, 2023, a U.S. federal court heard the case P.M. v. OpenAI LP, in which an anonymous group of plaintiffs filed a lawsuit against OpenAI LP (OpenAI) and Microsoft, Inc. (Microsoft). The plaintiffs alleged that OpenAI had misappropriated the personal and proprietary information of millions of individuals by collecting publicly available data from the Internet and social media platforms without users' knowledge or consent. They argued that OpenAI's practice of using such Internet-derived datasets to train its generative AI tools constituted theft, misappropriation, and violations of privacy and property rights. The allegedly collected information included names, addresses, phone numbers, email addresses, and financial data. According to the plaintiffs, OpenAI and Microsoft used this personal information to develop ChatGPT,

[55] Ibid, para 39.

[56] Access Alert: Peru's congress introduces bill to regulate AI, 2024, <https://accesspartnership.com/access-alert-perus-congress-introduces-bill-to-regulate-ai/> [05.05.2024].

[57] Peru Law - LAW THAT PROMOTES THE USE OF ARTIFICIAL INTELLIGENCE IN FAVOR OF THE ECONOMIC AND SOCIAL DEVELOPMENT OF THE COUNTRY, Unique item, f, <https://busquedas.elperuano.pe/dispositivo/NL/2192926-1> [05.05.2024].

thereby violating the U.S. Electronic Communications Privacy Act, which prohibits the interception of electronic communications without prior court authorization.

This case is particularly significant as it underscores the obligation of AI companies to ensure transparency in their data collection practices and to establish appropriate legal bases—such as obtaining user consent—before processing personal data. It also serves as a reminder that consumers should remain aware of the privacy implications associated with the use of AI products and services, including their potential exposure to copyright infringement issues and other forms of harm linked to AI-related data practices.[58]

On July 11, 2023, in the case J.L. v. Alphabet Inc., a class action lawsuit was filed in a U.S. federal court against Google, alleging violations of privacy and copyright laws. The plaintiffs claimed that Google's generative AI products—including Bard (a text generator), Imagen and Gemini (two text-to-image diffusion models), MusicLM (a text-to-music tool), and Duet AI (a data visualization tool)—relied on data that the company had collected from the Internet without proper authorization.[59]

The lawsuit further alleged that Google used online information for AI training purposes without obtaining consent from the original data owners. Specifically, it was claimed that Google's AI products utilized copyrighted text, music, images, and other materials for training purposes without the necessary permissions.[60]

The issue of using publicly available online information for artificial intelligence training had also been addressed in the U.S. court case hiQ Labs, Inc. v. LinkedIn Corp. In that case, hiQ Labs, Inc. "scraped" data from publicly available profiles of LinkedIn users to provide employers with insights about job seekers and employment trends. The court ruled that the use of publicly available data does not, in itself, constitute a violation of privacy rights. However, it emphasized that privacy would be infringed if an AI system used data that was not publicly accessible and had been granted the legal status of "personal data."[61]

Italy became the first Western country to temporarily block the chatbot ChatGPT due to privacy concerns. The Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) decided to suspend and investigate the chatbot—developed by OpenAI and supported by Microsoft—on the grounds that there was no legal basis to justify the collection and "mass storage" of personal data for the purpose of training the GPT AI modelThe Garante accused OpenAI of unlawfully collecting and retaining data of Italian data subjects, thereby violating the General Data Protection Regulation (GDPR). Additional concerns were raised about the lack of an effective age verification mechanism, which could expose minors to inappropriate content.

---

[58] Conexus law, OpenAI, and Microsoft sued in the US for §3 billion over alleged ChatGPT privacy violations, <https://www.conexuslaw.com/insight/openai-and-microsoft-sued-in-us-for-3-billion-over-alleged-chatgpt-privacy-violations/> [25.04.2024].

[59] J.L. et al. v. Alphabet Inc. et al. - 3:23-cv-03440

[60] *Christopher J. Valente, Stortz M.J., Wong A., Soskin P.E., Meredith M.W.,* US Litigation and Dispute Resolution Alert, 2023, <https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023> [25.04.2024].

[61] Ibid.

During the investigation, it was discovered that ChatGPT processed users' conversations, email addresses, and even the last four digits of their bank cards. According to the BBC, Italian authorities gave OpenAI 20 days to address these issues or face fines of up to 4% of its annual global revenue.[62] OpenAI denied the allegations. Ultimately, ChatGPT was temporarily blocked in Italy from March 31, 2023, to April 28, 2023, with the suspension lasting approximately four weeks (28 days).

Except for Italy, China has also taken restrictive measures against the use of ChatGPT. The Chinese government has banned the country's major technology companies from offering ChatGPT services to users. According to Nikkei Asia, the responses generated by the AI chatbot—developed by OpenAI and backed by Microsoft—would otherwise be subject to censorship by the Chinese Communist Party (CCP). Although ChatGPT is not officially available in China, some Internet users have managed to access it through virtual private networks (VPNs).[63]

The Hellenic Data Protection Authority (Hellenic DPA) imposed a €20 million fine on Clearview AI Inc. for violating the principles of lawfulness and transparency. The authority also prohibited the company from collecting or storing personal data within Greek territory without a valid legal basis. Clearview AI operates a facial recognition database in which personal data—specifically, photographs—are scraped from the Internet without the consent of the individuals concerned.[64]

Following Greece, the Austrian Data Protection Authority also issued a ruling against Clearview AI. The company reportedly maintains a database containing over 30 billion facial images sourced globally from publicly available materials such as media outlets, social networks, and online videos. It provides a sophisticated search service that enables artificial intelligence systems to generate profiles based on biometric data extracted from these images. These profiles can be further enriched with related information, including image tags, geolocation data, and source web pages, thereby heightening concerns about privacy, consent, and proportionality in the use of AI-driven facial recognition technologies.[65]

[62] ChatGPT was blocked in Italy, business formula <https://businessformula.ge/News/13437> [30.04.2024].

[63] *Papalashvili S., Nikkei Asia: China bans companies from using the ChatGPT service,* <https://forbes.ge/nikkei-asia-chinethi-kompaniebs-chatgpt-is-servisis-gamoqhenebas-ukrdzalavs/> [25.04.2024].

[64] Hellenic DPA fines Clearview AI 20 million euros, <https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en> [25.04.2024].

[65] Decision by the Austrian SA against Clearview AI Infringements of Article 5,6,9,27 GDPR, <https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en> [25.04.2024].

5. Conclusion

Although artificial intelligence and its regulation remain a relatively new reality for the global community, it is challenging to adopt definitive decisions regarding a system that continues to evolve and transform on a daily basis.

The processing of data by artificial intelligence may conflict with the fundamental requirements of the General Data Protection Regulation (GDPR)—particularly with respect to the principles of accountability, transparency, the existence of a lawful basis for data processing, and data minimization. Many AI applications involve the processing of personal data. On the one hand, such data may form part of the datasets used to train machine learning systems, particularly for the development of algorithmic models. On the other hand, these models can subsequently be employed to draw inferences about specific individuals based on personal data.

As this paper has demonstrated, legal instruments governing personal data protection exist at both the international and domestic levels. However, the key standards and principles for data protection and processing are primarily established by the General Data Protection Regulation, adopted by the Council of Europe, which sets a notably high standard for the protection of personal data. By contrast, the international legal framework governing artificial intelligence remains relatively new and largely untested in practice. The reviewed materials indicate that numerous countries have adopted recommendations, strategies, action plans, or policy documents addressing artificial intelligence at the national level. Nevertheless, it should be emphasized that these instruments are recommendatory in nature and lack binding legal force.

Bibliography:

1. European Convention on Human Rights, 1950, Articles 8 and 12.
2. European Union Artificial Intelligence Act (EU AI Act), para. 2.
3. European Union Artificial Intelligence Act (EU AI Act), para. 2.
4. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 1981.
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, OJ 1995 L 281.
6. General Data Protection Regulation (GDPR), Article 4(1).
7. General Data Protection Regulation (GDPR), Recital 26.
8. Law of Georgia on Personal Data Protection, 14 June 2023.
9. International Covenant on Civil and Political Rights (ICCPR), 1976, Article 17.
10. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 14.
11. Convention on the Rights of Persons with Disabilities, Article 22.
12. Access Alert: Peru's congress introduces bill to regulate AI, 2024, <https://accesspartnership.com/access-alert-perus-congress-introduces-bill-to-regulate-ai/> [05.05.2024].
13. Agency for Digital Government, The Danish National Strategy for Artificial Intelligence, <https://en.digst.dk/strategy/the-danish-national-strategy-for-artificial-intelligence/> [10.04.2024].
14. *Alfredsson G., Asbjorn E.*, The Universal Declaration of Human Rights A Common Standard of Achievement, Hague, Kluwer Law International, 1999, 257-258.
15. *Chalubinska-Jentiewicz K., Nowikowska M.,* Artificial Intelligence v. Personal Data, Polish Political Science Yearbook, vol 5., Poland 2022, 188-189.
16. Constitutional Court of Georgia, Decision No. 1/4/757 of 27 March 2017, Citizen of Georgia Giorgi Kraveishvili v. Government of Georgia, II-4.
17. Council of Europe, Consultative Committee of Convention 108, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 2.
18. Decision by the Austrian SA against Clearview AI Infringements of Article 5, 6, 9, 27 GDPR, <https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en> [25.04.2024].
19. *Dutton T.,* An Overview of National AI Strategies, Politics + AI 2018, <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> [10.03.2024].

20. EDPS, The History of the General Data Protection Regulation, <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> [15.01.2024].
21. European Commission, National strategies on Artificial Intelligence. A European perspective in 2019, Country report – Italy, <https://knowledge4policy.ec.europa.eu/sites/default/files/italy-ai-strategy-report.pdf> [17.04.2024].
22. European Commission, What is personal data? <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> [17.01.2024].
23. European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020, <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> [05.05.2024].
24. *Gabisonia, Z.,* Internet Law and Artificial Intelligence. Jurists' World, Tbilisi, 2022, 513, 526.
25. German Federal Government's AI Strategy, <https://www.bmwk.de/Redaktion/EN/Artikel/Technology/artificial-intelligence.html> [12.04.2024].
26. Government of Canada, The Artificial Intelligence and Data Act (AIDA)- Companion document, <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document?trk=article-ssr-frontend-pulse_little-text-block> [01.04.2024].
27. *Habuka H.*, Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency, Report 2023, <https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7 presidency#:~:text=As%20mentioned%20above%2C%20there%20are,occurs%20due%20to%20AI%20systems?trk=article-ssr-frontend-pulse_little-text-block> [30.03.2024].
28. India's National Strategy for Artificial Intelligence, 2018, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> [17.04.2024].
29. *Klimentov M.,* From China to Brazil, here's how AI regulated around the world, September 2023, <https://www.washingtonpost.com/world/2023/09/03/ai-regulation-law-china-israel-eu/?trk=article-ssr-frontendpulse_little-text-block> [25.03.2024].
30. *Kohn B.,* Pieper F.U., AI Regulation around the World, 2023, <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/ai-regulation-around-the-world> [20.03.2024].
31. National Artificial Intelligence Strategy 2.0 to Uplift Singapore's Social and Economic Potential, 2023, <https://www.smartnation.gov.sg/media-hub/press-releases/04122023/> [15.04.2024].

32. National Strategy for Artificial Intelligence of Korea, https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10&mPid=9 [15.04.2024].
33. Navigating the Future Malaysia's Ethical AI Vision, <https://thesun.my/business/navigating-the-future-malaysia-s-ethical-ai-vision-IP12485793> [29.05.2024].
34. OECD Recommendation of the Council on Artificial Intelligence, 2024.
35. OVIC, Artificial Intelligence and Privacy – Issues and Challenges, <https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/> [05.05.2024].
36. *Papalashvili, S. Nikkei Asia: China Prohibits Companies from Using ChatGPT Services. Retrieved from* <https://forbes.ge/nikkei-asia-chinethi-kompaniebs-chatgpt-is-servisis-gamoqhenebas-ukrdzalavs/> [25.04.2024].
37. Poland AI Strategy Report, <https://ai-watch.ec.europa.eu/countries/poland/poland-ai-strategy-report_en> [18.04.2024].
38. *Prinsley M.A., Yaros O., Randall R., Hajda O., Hepworth E.,* UK's Approach to Regulating the Use of Artificial Intelligence, <https://www.mayerbrown.com/en/insights/publications/2023/07/uks-approach-to-regulating-the-use-of-artificial-intelligence> [10.04.2024].
39. *Russel S., Norvig P.*, Artificial Intelligence: A Modern Approach (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2003, 27, 32–58, 968–972.
40. Scientific Journal "Young Lawyers", No. 5. Joint publication of "Young Lawyers" and the "Lawyers' Educational Center", Tbilisi, 2016, 34.
41. Stuart Russel and Peter Norvig, Artificial Intelligence: A Modern Approach (3rd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2009, 2.
42. UAE National Strategy for Artificial Intelligence 2031, <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf> [15.04.2024].
43. *Valente Ch. J.*, Stortz M.J., Wong A., Soskin P.E., Meredith M.W., US Litigation and Dispute Resolution Alert, 2023, <https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023> [25.04.2024].

Giorgi Khorbaladze[*]

Processing of Personal Data of a Data Subject through Disclosure on Social Networks

The development of information technologies, while offering numerous opportunities, has also introduced significant risks, particularly those affecting the right to privacy. Data processing in the online environment is becoming increasingly widespread. Of particular importance is the processing of personal data through disclosure on various social networks and digital platforms. Such processing is not considered unlawful provided that it complies with the requirements of personal data protection legislation.

The purpose of this paper is to examine, through practical examples, the specific characteristics of data processing by means of disclosure on social networks and to identify the conditions and criteria under which such processing may be deemed lawful.

Keywords: *Data subject, data controller, data processing, social networks.*

1. Introduction

With the rapid development of information technologies, the legality of personal data processing has become an increasingly relevant issue. Despite the inherent challenges, risks, and threats associated with automated data processing, data subjects often publish their personal information online without considering the possibility of unwanted processing by others. When their rights are violated, they may seek remedies through the relevant authorities, authorized persons, or the courts.

The Law of Georgia "On Personal Data Protection" does not provide an exhaustive list of forms of data processing; any action performed on personal data is, in itself, considered processing. This study does not aim to provide a comprehensive review of all forms of data processing on social networks. Rather, it focuses on the most common form: the disclosure, publication, distribution, or otherwise making personal data publicly available online. The scope of this study is further narrowed by focusing on the identification of the data controllers, specifically examining cases

[*] Master of Laws (LL.M.), Ivane Javakhishvili Tbilisi State University; Senior Lawyer of Presidents Office, Personal Data Protection Service of Georgia.

where individuals, rather than public or private institutions, process personal data. This focus is justified by the fact that national data protection legislation allows individuals to process personal data for clearly personal purposes and/or within the context of family activities without being fully bound by the requirements of the Law of Georgia on Personal Data Protection. Consequently, this study highlights cases where the right to privacy and personal data protection takes precedence over other rights and explores how the law applies to specific instances of individual data processing.

The paper analyzes the legal aspects of personal data processing by individuals on social networks through disclosure, drawing on theoretical frameworks, relevant practices of the Personal Data Protection Service, approaches of data protection supervisory authorities, and case law from the European Court of Human Rights. In addition, it examines the legal basis for processing personal data on social networks, instances of data processing within entrepreneurial and economic activities, features of processing during professional activities or official duties, and processing for clearly personal or family-related purposes.

2. Legal Basis for Processing Personal Data through Social Networks

The requirements of the Law of Georgia on Personal Data Protection do not apply to natural persons who process personal data for clearly personal purposes and/or within the context of family activities. Under current legislation, such processing may include a natural person's online activity on social networks. However, in certain cases, a natural person may still be subject to the Law on Personal Data Protection when their actions on social networks fall within entrepreneurial, economic, professional, or official duties. For example, if an individual discloses another person's personal data on a social network while simultaneously acting in a professional or business capacity, the law will apply, and the individual will be considered the data controller or data processor.

If the processing by a natural person does not fall within the statutory exceptions, the data controller is obliged, during an examination by the Personal Data Protection Service, to justify the legal basis for processing in accordance with Articles 5 or 6 (in the case of special categories of data) of the Law on Personal Data Protection.

A universal legal basis for processing personal data is the oral or written (including electronic) consent of the data subject, when the data are obtained directly from them. However, if the consent does not specifically authorize the controller to disclose the data on a social network, the processing will be considered incompatible with the original purpose. In such cases, the controller must rely on another legal basis provided by law. It is difficult to envisage a scenario where the data subject's consent would justify disclosure on a social network if the data subject objects to the processing.

Of particular interest is the case in which the processing of personal data is based on the circumstance that the data subject has previously made their own data public, and in the case of special categories of data, has done so without an explicit prohibition on use. In this regard, one case studied by the Personal Data Protection Service during an unplanned inspection, concerning data processing on the above-mentioned grounds, is particularly relevant. According to the circumstances of the case, the data subject posted a video on the social network TikTok in which they discussed the benefits of a certain product. Part of the distributed video, which contained the applicant's personal data (visual image and voice), was reposted by a natural person who owns accounts on Facebook, Instagram, and TikTok. The applicant explained that the account owner used the video containing their personal data for commercial purposes (product advertising) without permission, posting it on their own TikTok account, which had more than 500,000 followers. According to the controller, they were selling the product advertised by the data subject online and posted the video containing the applicant's personal data on various social media accounts to inform the public about the product's availability in Georgia. As a result of the investigation, the Personal Data Protection Service established that the applicant had activated the sharing, as well as the "Duet" and "Stitch" functionalities on the video they posted, which allowed another account owner to create a new video using the original video clip or its fragment. The Service noted that, when posting the video, the applicant should have been aware of the risk that the video could become publicly available and potentially be further processed. It was determined that the data processing was based on the provision in subparagraph "e" of paragraph 1 of Article 5 of the Law, as the data subject had made their personal data publicly available. Accordingly, no violation of the requirements of the Law "On the Protection of Personal Data" was detected in the processing of the applicant's data by a natural person on various social networks.[1]

The publicity of data may also arise from legislation. For example, according to Article 6, Paragraph 1 of the Law of Georgia "On Public Registry,"[2] data registered in the public registry and documentation maintained by the registering authority are considered public. Similarly, the Law of Georgia "On Entrepreneurs"[3] provides for the publicity of certain data. The requirement to make data public may serve purposes such as ensuring the stability of civil turnover. However, regardless of the legislator's objective, the processing of such data should not come as a surprise to the data subject.

In individual cases, the processing of personal data may serve to protect the legitimate interests of the controller or a third party, except where those interests are overridden by the overriding interest of protecting the rights of the data subject,

[1] Decision of the President of the Personal Data Protection Service, No. G-1/107/2025, 3 April 2025 (obtained from the Service as public information).
[2] Law of Georgia on the Public Registry, 820, 19/12/2008, Article 6, Paragraph 1.
[3] Law of Georgia on Entrepreneurs, 875-Vრს-Xმპ, 02/08/2021, Article 13, Paragraph 1.

including minors.[4] The legitimacy of the controller's purpose and the necessity of data processing must be assessed on a case-by-case basis, balancing the interests of all parties to reach a lawful and fair decision. In this context, the Personal Data Protection Service considered a case concerning the disclosure of a data subject's personal data by a natural person on the social network Facebook. According to the circumstances, the parties had concluded an oral agreement in which the data subject, in the context of his entrepreneurial activity, undertook to send vehicles from the People's Republic of China to Georgia for a certain fee to the data controller. The controller argued that the data subject violated the terms of the agreement, as the vehicles consisted of secondary materials/parts and could not be operated. Communication with the applicant to resolve the issue had been unsuccessful. Within the investigation, it was revealed that the controller published the applicant's personal data in the form of a post and screenshots on his personal Facebook account and in one public group. These screenshots included the applicant's Facebook profile page, displaying their name, surname, two photographs (profile and cover photos), and part of their passport photograph. The controller explained that the purpose of disclosing the data was not to discredit or blackmail the applicant but to protect his own interests. Since the applicant had caused material damage to multiple people, the controller aimed to prevent further harm, thereby asserting a legitimate interest in protecting his own and third parties' material interests and informing the public. Accordingly, the controller considered the information disseminated to be proportionate and minimal. He also cited the exercise of his right to freedom of expression. The Personal Data Protection Service recognized the legitimacy of the controller's interest but found that the processing of the applicant's data did not meet the "necessity" criterion. Although the applicant had made some information publicly available on Facebook, creating a legal basis for processing, the controller could have achieved his purpose by less intrusive means, without publishing a screenshot of the applicant's passport. Therefore, despite the right to freedom of expression, the controller was obliged to pursue the protection of property interests and public information in a manner proportionate to the data subject's right to privacy. Based on this assessment, the Service determined that Article 5 of the Law had been violated and imposed an administrative penalty on the controller under Article 67 of the Law.[5]

The Law of Georgia on Personal Data Protection requires that a controller process personal data based on at least one of the legal grounds, an exhaustive list of which is set out in Articles 5 and 6 of the Law. The burden of proving the legal basis for any data processing operation rests with the controller, and its relevance is assessed by the Personal Data Protection Service during the examination of the lawfulness of the processing.

[4] Law of Georgia on Personal Data Protection, 3144-XIმს-Xმპ, 14/06/2023, Article 5, Paragraph 1, Subparagraph "i".

[5] Decision of the Head of the Personal Data Protection Service, No. G-1/259/2025, 23 July 2025 (obtained from the Service as public information).

3. Data Processing within the Framework of Entrepreneurial and Economic Activities

Entrepreneurial activity is a lawful, non-recurring, independent, and organized activity carried out for the purpose of making a profit. It can be conducted either as an individual entrepreneur or as an entrepreneurial society[6]. Economic activity is defined as any activity undertaken to receive income or compensation, regardless of the outcome. [7] Data processing by a natural person within the framework of these activities is not considered an exception to the scope of the Law "On Personal Data Protection." In such cases, the data processing must fully comply with the legal requirements established by the Law.

The Personal Data Protection Service, acting on a notification from the Public Defender's Office of Georgia, examined a case concerning the processing of minors' data on a Facebook page. In this case, data controller registered in the Register of Entrepreneurs and Non-Entrepreneurial Legal Entities as an individual entrepreneur, managed the Facebook page and posted a call to parents or legal representatives of minors to upload photographs of minors in the comments section in order to participate in a photo contest. According to the controller, the contest winner would be determined by the number of "likes" on each photograph and by a specific electronic program at random. It was established that some of the submitted photographs of minors, including images containing naked children, remained publicly accessible on the page even after the contest ended. The Personal Data Protection Service determined that, since the individual was conducting these activities as an individual entrepreneur, the Law on Personal Data Protection applied to the data processing. Although the photographs were posted by parents or legal representatives, the individual was considered the data controller, as he automatically collected and displayed the participants' photos in the course of his entrepreneurial activity. Despite the parents' consent to post the photographs, the Personal Data Protection Service issued a mandatory instruction to data controller requiring the deletion of the photographs and associated comments from the post, in line with the best interests of the minors. In the event of a similar future competition, the controller is required to perform the same deletion task after achieving the relevant goal.[8]

An interesting case arises when it is not the controller who acts within the scope of professional activity, but the data subject themselves, and the processing of data is related to the performance of their official duties. The European Court of Human Rights considered the case Toth and Crișan v. Romania,[9] in which, on 8 April 2016,

[6] Law of Georgia on Entrepreneurs, 875-Vრს-Xმპ, 02/08/2021, Article 2, Paragraphs 2 and 3.

[7] Law of Georgia on the Tax Code, 3591, 17/19/2010, Article 9, Paragraph 1. Approved by the National Statistics Office of Georgia according to the types of economic activities defined in the National Classifier of Georgia. See: <https://www.geostat.ge/media/70150/NACE-Rev_2_GE_2023.pdf> [30.8.2025].

[8] Decision of the Head of the Personal Data Protection Service, No. G-1/269/2025, 1 August 2025 (obtained from the Service as public information).

[9] Case of Toth and Crișan v. Romania, [2025] ECHR, App. No. 45430/19.

police officers (the applicants) fined S.T. and his mother for violating household waste disposal rules. On the same day, S.T., using his personal Facebook account, published a post in a public group, accompanied by a photograph of the applicants taken at the scene. The post described the incident and alleged that the police officers had physically assaulted the mother and daughter in the presence of the child and verbally abused them. The post was followed by responses from group members. In the comments, Facebook users referred to the complainants with derogatory terms (e.g., "idiots," "crazy," "uneducated"), and some identified the officers, citing similar incidents. In his comments, S.T. revealed the name of one of the complainants and stated that he did not intend to defame them.

The applicants applied to the domestic court seeking compensation for non-pecuniary damage and requiring S.T. to issue an apology to local newspapers and the public group, as he had published the photograph and name of one of the applicants without consent. This had led to offensive comments by others and disciplinary proceedings against the applicants by their employer. The domestic courts dismissed the claims, finding that the post was not defamatory, that it conveyed S.T.'s own perception of the event, and that it constituted an exercise of his right to freedom of expression by publicly sharing his dissatisfaction. The courts further held that S.T. could not be held responsible for comments posted by others, which he could not delete or prevent, and that the photograph and names had been publicly distributed. Moreover, the applicants, as public figures, were not depicted in an indecent manner.

The applicants then brought the case before the European Court of Human Rights, alleging a violation of Article 8 of the European Convention on Human Rights. The Court noted that the publication of a photograph constitutes a more substantial interference with the right to respect for private life than the mere disclosure of a name. However, if the publication does not concern political or public debate and relates solely to private matters intended to satisfy personal curiosity, the right to freedom of expression is interpreted more narrowly. The Court outlined the relevant criteria for balancing the right to privacy and freedom of expression: contribution to matters of public interest; the notoriety of the affected person; the person's previous behavior; and the circumstances of taking the photograph, including the content, form, and consequences of the published information. The Court found the publication of the photograph justified, as it confirmed the information presented in the post. Unlike the national courts, the European Court did not consider the applicants to be public figures in the strict sense, but noted that given their roles and activities, they were subject to broader permissible criticism. Accordingly, the public had the right to receive information about professionals serving the community, and the applicants should have expected that, given their status and conduct, their photographs could be taken and further processed. The Court ultimately found no violation of Article 8 of the European Convention on Human Rights.

4. Data Processing in Social Networks in the Course of Professional and Official Duties

The processing of personal data in the course of a person's professional or official duties falls within the scope of the Law of Georgia on Personal Data Protection.

The Personal Data Protection Service examined a case concerning the publication of a video recording of correspondence between individuals on the social network Facebook. In this case, the data subject had entered into an agreement with a composer, under which the composer was to write a song in exchange for remuneration. Due to a violation of the terms of the agreement, the composer, as the data controller published a video recording of the communication on his personal Facebook page. The controller explained that the purpose of publishing the video was to inform the public about the applicant's alleged fraudulent activities and to recover the royalties owed. The Service determined that the publication was related to the professional activities of the controller. However, it concluded that the action did not meet the "necessity" criterion defined in subparagraph "i" of paragraph 1 of Article 5 of the Law, as the composer could have protected his rights without infringing on the data subject's rights—for example, by pursuing legal action. Furthermore, the legitimate interests of third parties and the prevention of non-fulfillment of contractual obligations could have been safeguarded by including appropriate terms in the contract. Based on Article 67 of the Law, the Service imposed administrative liability on the controller and ordered the removal of the video recording containing the applicant's personal data from Facebook.[10]

In another case, the Service assessed the publication of a client's data by a real estate agent in a closed Facebook group of approximately 128,000 members. The agent, as the data controller explained that he had published information about his business relationship with the applicant—including the applicant's name, surname, telephone number, and photo obtained via WhatsApp—to inform colleagues about an allegedly unscrupulous client. The Service determined that, although the data were obtained within the framework of a professional relationship, they did not constitute a professional secret, as no confidentiality agreement existed between the parties. Moreover, the agent could not substantiate a legal basis for processing the data. As a result, the Service found the agent in violation of Article 5 of the Law.[11]

In a further case, an anonymous post in a closed Facebook group included the name and surname of the applicant. An employee of a company subsequently posted a comment in the same thread, clarifying the facts referenced in the anonymous post and naming the applicant as the main figure in the event. The Service assessed the processing of the applicant's data in the comment independently of the anonymous post. It was established that the employee was the head of the company's security service and that his employment contract included an obligation to maintain

[10] Decision of the Head of the Personal Data Protection Service, No. G-1/183/2025, 3 June 2025 (obtained from the Service as public information).

[11] Decision of the Acting Head / First Deputy Head of the Personal Data Protection Service, No. G-1/374/2024, 19 December 2024 (obtained from the Service as public information).

confidentiality. The company and the controller clarified that the comment was posted independently and was not based on company instructions, and that the disclosed information had not been obtained in the course of official duties. The controller also failed to specify a legal basis for the data processing. Consequently, the Service determined that there was no lawful basis for publicly processing the applicant's data and imposed an administrative penalty on the company employee under Article 67 of the Law.[12]

5. Data Processing for a Clearly Personal Purpose and in the Context of Family Activity

The processing of personal data by a natural person for a clearly personal purpose and/or within the context of family activity, as an exception from the scope of personal data protection legislation, was first introduced by the European Union Directive 95/46/EC of 24 October 1995.[13] Following the repeal of that Directive, the same exception was incorporated into the European Union's General Data Protection Regulation (GDPR).[14] A similar provision is reflected in the Law of Georgia On the Protection of Personal Data, which stipulates that the Law does not apply to data processing carried out by a natural person for a clearly personal purpose and/or within the context of a family activity, provided that such processing is not related to entrepreneurial and/or economic, professional activity, or the performance of official duties. Data processing for a clearly personal or family-related purpose may include, among others, personal correspondence, management of contact information, and internet activity (including on social networks) carried out within the scope of such activity.[15]

"When posting on the Internet, a person must understand that he or she loses control over his or her own photo, notes, and/or other personal data."[16] In today's digital environment, the processing of personal data through social networks has become increasingly widespread alongside the advancement of information technologies. Individuals themselves are often the initiators of various data processing activities. It is therefore impossible to consider every instance of online data publication as an unconditional violation of personal data protection legislation. Where the disclosure of personal data on social networks arises from a person's

[12] Decision of the Head of the Personal Data Protection Service, No. G-1/307/2024, 24 October 2024 (obtained from the Service as public information).

[13] European Union Directive 95/46/EC of 24 October 1995, OJ L 281, 23/11/1995, Article 3. See: <https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng> [18.9.2025].

[14] European Union General Data Protection Regulation (GDPR), OJ L 119, 4/5/2016, Preamble, Paragraph 18. See: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> [18.9.2025].

[15] Law of Georgia on Personal Data Protection, 3144-XIმს-Xმპ, 14/06/2023, Article 2, Paragraph 2, Subparagraph "a".

[16] *Macuka Y.*, Director of DVI, interview with "LSM", <https://shorturl.at/pKZlH> [14.9.2025].

entrepreneurial, commercial, professional, or service-related activity, the supervisory authority, in accordance with the Law of Georgia On Personal Data Protection, will assess the lawfulness of such processing. In all other cases, the extent to which the processing is "necessary" for achieving the legitimate purpose of the data controller must be assessed individually, based on a range of relevant criteria.

According to the circumstances of one of the cases reviewed by the Personal Data Protection Service, a patient visited a clinic to receive medical services. Dissatisfied with the services provided, he photographed the medical staff and publicly posted the images on the "Google Reviews" platform along with a negative comment. The Service determined that the individual had disseminated personal data online in order to publicly express his opinion, attitude, and assessment regarding the clinic's services, and that the data had not been processed within the framework of entrepreneurial, economic, or professional/service activities. The Service also explained that the legal norms[17] regulating defamation and the protection of personal dignity could potentially apply to the given case. The Civil Code of Georgia protects personal non-property rights, which also encompass information disseminated through social networks. [18] As noted in the law, "Information disseminated by a person through social networks—expressed opinions or recorded data—may violate the rights of others."[19]

Publicly disclosing another person's personal data on social networks and making it accessible to all users does not constitute data processing for a personal purpose and/or within the framework of family activity. This exception applies, for example, to private correspondence conducted via social networks or the sharing of data with close friends or family members, where the personal data of others does not become available to the general public. For the exception to apply, it is essential to assess the number of data recipients. Accordingly, the public disclosure of personal data by an individual—regardless of whether the person acted within a commercial or professional context—immediately excludes the possibility that the data was processed for personal or family purposes. In such cases, the supervisory authority is entitled to examine the lawfulness of the processing. However, within the limits of its mandate, if it is determined that the natural person data controller was clearly exercising the right to freedom of expression (for instance, by expressing a personal opinion or sharing an experience), the supervisory authority may decline to consider the complaint. In such circumstances, the affected party must apply to the court to seek protection of their rights—such as honor, dignity, privacy, personal inviolability, or business reputation—which will often need to be balanced against the counterparty's right to freedom of speech and expression.

[17] Correspondence of the Official Responsible for Ensuring Public Access to Information of the Personal Data Protection Service, No. PDPS 3 25 00015900, 17 September 2025 (obtained from the Service as public information).

[18] Civil Code of Georgia, 786, 26/06/1997, Article 18.

[19] Commentary on the Civil Code, Book I, General Provisions of the Civil Code, Tbilisi, 2017, 112. See: <https://lawlibrary.info/ge/books/giz2017-ge-civil_code_comm_I_Book.pdf> [20.9.2025].

Assessing whether an individual has exceeded the limits of the right to freedom of expression does not fall within the competence of the supervisory authority. This approach was also reflected in the practice of the Icelandic Data Protection Authority, which declined to examine the lawfulness of publishing photographs of a minor on the social network "Facebook." According to the circumstances of that case, a dispute had arisen between the child's parents concerning custody. One of the parents, together with a third party (another social network user), published photographs of the minor on the same platform accompanied by defamatory comments about the other parent. The supervisory authority found that the child was identifiable in the photographs and that, under the GDPR, the publication of both the image and the accompanying comments constituted data processing. The authority concluded that the case did not fall within the scope of personal or family-related data processing, explaining that this exception applies only to closed social network accounts, where posts are accessible to a limited audience rather than the general public. It was established that the child's data had been made accessible to all Facebook users without any restrictions. Accordingly, the GDPR applied to the case. At the same time, the supervisory authority found that the parent who had published the child's data was exercising the right to freedom of expression—namely, by informing the public about his difficult situation related to the custody dispute. On the grounds that it lacked the competence to rule on the restriction of constitutionally guaranteed freedom of expression, the authority determined that the matter was subject to judicial review. Consequently, it rejected the complaint concerning the processing of the child's data on the social network by the parent and the third party.[20]

The Personal Data Protection Service did not consider the processing of another person's personal data by a natural person, through the publication of a video recording on the social network "Facebook," as data processing for a clearly personal purpose. According to the circumstances of the case, the natural person had used the courier service of a company to order food products. Dissatisfied with the company's service due to the late delivery of the order, the customer refused to accept it and recorded a video clip containing the courier's visual image in order to document the complaint. The data contoller subsequently posted the video on his publicly accessible Facebook page. He explained that the purpose of creating and publishing the video clip in a publicly accessible form was to record a claim against the company, not to directly insult the courier. The Service clarified that an action cannot be regarded as being carried out in the context of a clearly private or family activity when its purpose is to make the collected data accessible to an unlimited number of persons. Furthermore, the exception does not apply in cases where the action or activity is at least partially directed toward the public sphere and extends beyond the personal or family context of the data controller. The decision emphasized that while the use of

[20] Decision of the Icelandic Data Protection Authority, No. 2020010552, 17 November 2021. See: <https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_(Iceland)_-_no._2020010552> [30.8.2025].

social networks and online activities may fall within the context of personal or family activities, this is only applicable when data exchange occurs within closed groups, without any connection to professional or economic activities. Exclusively private use of such services falls within the scope of the exception, provided that it does not involve the unrestricted publication of personal data on the Internet. The Service also assessed the existence of an important legitimate interest of the data controller and the necessity of data processing to protect that interest (noting that processing is considered "necessary" only when there is no other, less intrusive means of protecting a legitimate interest). The individual data controller failed to substantiate a legal basis for posting the personal data of the courier in a publicly accessible form on his Facebook page. The Service explained that the person had alternative ways to express dissatisfaction with the company that would have resulted in less interference with the courier's right to personal data protection — for instance, by posting the video in a restricted-access format visible only to a limited circle of people, within a closed group, or by contacting the company directly in written form to submit a complaint. Accordingly, the Service found a violation of Article 5 of the Law ("Legal Basis for Processing").[21]

Based on the above definitions, it is evident that data processing for a clearly personal purpose and/or within the framework of family activities cannot be considered to exist when personal data are made accessible to an indefinite number of persons.[22] For example, the publication of a data subject's health information by a natural person on a social network—regardless of the scope of that person's activities—will fall within the scope of the Law. In such cases, the supervisory authority must assess whether there was a lawful basis for processing the data in this manner. In individual cases, the supervisory authority should also assess whether the matter is wholly or partly related to the exercise of the right to freedom of expression by the data contoller. For instance, factors such as the social nature of the processing, any prior relationship between the parties, and the connection between the act of processing personal data and an existing legal dispute may be relevant to this assessment.

Taking into account the approaches established by the Law on Personal Data Protection, it is therefore possible to identify several criteria to guide supervisory authorities in properly assessing such cases.[23] In particular, supervisory authorities should determine whether data processing by a natural person falls within the scope of personal and/or family activities by applying the following criteria:

[21] Decision of the Head of the Personal Data Protection Service, No. G-1/355/2025, 23 September 2025 (obtained from the Service as public information).

[22] According to EU case law, if the purpose of a natural person is to make collected data available to an unlimited circle of persons, then it is not considered data processing for a clearly personal purpose. See: <https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].

[23] See:<https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].

- **Data processing environment** – the dissemination of data to an indefinite number of persons through social networks does not constitute processing for a personal purpose;
- **Social context of processing –** the environment in which the individual processes personal data should be taken into account, including the nature of the data subjects and the group of persons who have access to the disseminated information;
- **Necessity of processing –** the processing must be necessary to achieve a legitimate purpose pursued by the individual, such as the exercise of the right to freedom of expression;
- **Nature of the individual's activity –** the processing of personal data carried out within the framework of economic, entrepreneurial, professional, or service-related activities does not qualify as data processing for personal purposes.

6. Conclusion

The development of information technologies, while offering numerous opportunities, has also introduced risks that may impede the effective exercise of personal autonomy and the right to privacy. Data processing in the online space is becoming increasingly widespread, and social network users often share personal data with a wide audience without fully considering the potential risks of unauthorized processing by others. While sharing personal data on social networks is common and often seen as relevant today, it may, from a future perspective, be regarded as imprudent or inconvenient. As noted, "In the Internet space, it is difficult, painful, and sometimes even impossible to delete one's personal data."[24]

When making personal data public, data subjects must exercise utmost caution, as further unauthorized or unwanted processing may conflict with the Law on the Protection of Personal Data. Data protection legislation grants the controller the right to process personal data, for example, when the data subject has voluntarily made such data publicly available. The rights to privacy, family life, private space, and communication are not absolute and may be limited by law or to protect the rights of others. In a democratic society, the competing nature of human rights necessitates a fair balance between individual rights, and it is unjustifiable to safeguard the interests of one party at the expense of another. The limitation of personal data protection legislation to cases of data processing by a natural person for a clearly personal and/or family purpose reflects this aim of maintaining such a balance. The legislator explicitly excluded data processing for personal purposes and/or within family activities from the scope of entrepreneurial, economic, professional, or official duties.Furthermore,

[24] See: <https://www.facebook.com/photo/?fbid=1094114552832861&set=a.181886710722321> [14.9.2025].

national and international data protection practice confirms that the disclosure of other persons' personal data by a natural person on social networks does not constitute data processing for a clearly personal purpose. Consequently, the lawfulness of such actions must be assessed under personal data protection legislation. Importantly, while processing personal data by a natural person through disclosure on social networks often falls within the scope of the Law on Personal Data Protection, it does not automatically imply illegality. Legal grounds for such processing, as provided under the Law of Georgia on Personal Data Protection, may apply, and each case should be assessed based on its specific circumstances.

Bibliography:

1. Law of Georgia on Personal Data Protection, 3144-XIMS-XMP, 14/06/2023.
2. Civil Code of Georgia, 786, 26/06/1997.
3. Law of Georgia on Entrepreneurs, 875-Vრს-Xმპ, 02/08/2021.
4. Law of Georgia on the Tax Code, 3591, 17/19/2010.
5. Law of Georgia on the Public Registry, 820, 19/12/2008.
6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.
7. Commentary on the Civil Code, Book I, General Provisions of the Civil Code, Tbilisi, 2017, 112.
8. Correspondence of the Official Responsible for Ensuring Public Access to Information of the Personal Data Protection Service, No. PDPS 3 25 00015900, 17 September 2025 (obtained from the Service as public information).
9. Decision of the Acting President / First Deputy President of the Personal Data Protection Service, No. G-1/374/2024, 19 December 2024 (obtained from the Service as public information).
10. Decision of the President of the Personal Data Protection Service, No. G-1/355/2025, 23 September 2025 (obtained from the Service as public information).
11. Decision of the President of the Personal Data Protection Service, No. G-1/269/2025, 1 August 2025 (obtained from the Service as public information).
12. Decision of the President of the Personal Data Protection Service, No. G-1/259/2025, 23 July 2025 (obtained from the Service as public information).
13. Decision of the President of the Personal Data Protection Service, No. G-1/183/2025, 3 June 2025 (obtained from the Service as public information).
14. Decision of the President of the Personal Data Protection Service, No. G-1/107/2025, 3 April 2025 (obtained from the Service as public information).
15. Decision of the President of the Personal Data Protection Service, No. G-1/307/2024, 24 October 2024 (obtained from the Service as public information).

16. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995.
17. *Case of Toth and Crișan v. Romania*, ECHR, App. No. 45430/19, 2025.
18. Persónuvernd (Iceland) - no. 2020010552 [17.11.2021] (<https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_(Iceland)_-_no._2020010552> [30.8.2025]).
19. <https://gdprhub.eu/index.php?title=Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity> [19.9.2025].
20. <https://www.facebook.com/photo/?fbid=1094114552832861&set=a.181886710722321> [14.9.2025].
21. <https://shorturl.at/pKZlH> [14.9.2025].

PERSONAL DATA
PROTECTION SERVICE

Address: №7 Nato Vachnadze, Tbilisi, 0105
№48, Baku Street, Batumi, 6010
www.pdps.ge
Tel.: (+995 32) 242 1000
E-mail: office@pdps.ge