PERSONAL DATA
PROTECTION SERVICE

JOURNAL OF PERSONAL DATA PROTECTION LAW

N2, 2024

PERSONAL DATA
PROTECTION SERVICE

Journal of Personal Data Protection Law

№2, 2024

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

Table of Contents

From the Editor-in-Chief

We are pleased to present the latest edition of the *Journal of Personal Data Protection Law*, which reflects the rapidly evolving challenges in the field of privacy and examines current developments in data protection law.

Over the past decade, significant efforts have been made to establish uniform regulation and consistent practice in the protection of the fundamental right to data protection. In Georgia, this right is enshrined in Article 15 of the Constitution, which safeguards the rights to personal and family privacy, personal space and privacy of communication. Any restriction of these rights is permissible only in accordance with the law—either with a court order or, in cases of urgent necessity defined by law, without prior judicial authorization. In such urgent cases, however, the court must be promptly informed and must subsequently confirm the legality of the restriction.

In the digital era, where rapid technological development and transparent data exchange continually raise new legal and ethical challenges, it is essential for public awareness to keep pace with the undeniable need to protect fundamental human rights amidst technological progress. One of the most effective ways to safeguard the right to personal data—and to enhance public understanding of this right—is through legal discourse on current issues related to personal data processing. The scientific Journal of the Personal Data Protection Service of Georgia is dedicated to fulfilling this purpose.

This issue of the Journal offers readers in-depth legal analysis and insights on a range of topical issues in the field of personal data protection. The published works address subjects such as the interpretation and implementation of European data protection standards, the role and activities of supervisory authorities, and the evolving legislative frameworks in response to technological transformation etc.

A particularly notable contribution comes from Professor Norbert Bernsdorf of the Philipp University of Marburg—retired judge of the German Federal Social Court and a member of this Journal's editorial board—whose article examines personal data protection in the context of electronic commerce. The paper provides a detailed discussion of the EU *Digital Services Act* and its implementation into national legislation. This analysis is especially relevant in light of the new obligations imposed on digital service providers, which have

significant implications for the protection of data subjects' rights. I would like to extend my sincere gratitude to Professor Bernsdorff for his continued scientific contributions to this Journal and for his active collaboration with the Personal Data Protection Service of Georgia.

Another scientific article is co-authored by Professor Thomas Hören, Director of the Institute for Information, Telecommunications and Media Law at the University of Münster; Philipp Mayer, Research Assistant at the same institution; and Gesa Schenke, Research Assistant at an international law firm. Their article explores the essence and scope of the principle *Poena Sine Culpa* in personal data protection law, and provides an analysis of the recent Court of Justice of the European Union (ECJ) ruling in the *Deutsche Wohnen* case—an important decision concerning the lawfulness of data processing and the protection of data subjects' rights.

The scientific article by Dr. Otar Chakhunashvili—Assistant Professor at the Faculty of Law, Ivane Javakhishvili Tbilisi State University, and First Deputy President of the Personal Data Protection Service of Georgia —focuses on the principles governing administrative offense proceedings in the context of evaluating the lawfulness of personal data processing. The work outlines the key legal principles that guide the Service's assessment of data processing practices.

From a practical perspective, a highly engaging contribution comes from practicing lawyer Dr. Sergi Jorbenadze, Associate Professor at the Faculty of Law, Ivane Javakhishvili Tbilisi State University. His paper addresses personal data processing in the context of lawyers' legal practice and presents recent legislative standards and practices developed by the Personal Data Protection Service of Georgia.

Against the backdrop of modern technological progress, employees of the Personal Data Protection Service of Georgia address several topical issues in their articles, including data processing through cloud systems, video surveillance of employees' workspaces and activities, the legal regulation of artificial intelligence systems and associated data protection challenges, as well as data protection in the context of academic research.

I would like to express my heartfelt appreciation to each author for their invaluable contributions to this publication. The overarching goal of the Journal is to enhance data protection standards and promote public awareness. Each article holds significant value for professional discourse and contributes meaningfully to the public's legal education. We hope that, given the scientific and practical importance of the featured works, this edition will serve as a valuable resource for legal professionals, researchers, and a broader readership interested in the evolving landscape of personal data protection.

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

Norbert Bernsdorff*

E-Commerce and Data Protection - The Digital Services Act and its National Implementation

As part of a "European data strategy", the European Commission has long been endeavouring to create a uniform European internal data market and to establish new regulations for the use of artificial intelligence. In the area of conflict between the requirements of Article 8 of the Charter of Fundamental Rights of the European Union on data protection on the one hand and the need to facilitate the handling of personal data - which is important for the digital economy - on the other, several laws proposed by the European Commission (Data Governance Act, Data Act, Digital Services Act and Digital Markets Act) have created the necessary framework conditions. The Digital Services Act in particular regulates the new obligations for providers of digital services.

Keywords: *Data protection on the internet, Digital Services Act, internal data market, E-Commerce, digital services, transmission-, caching- and hosting-services, online platforms, imprint obligation, General Data Protection Regulation.*

1. Introduction

Digital services influence and facilitate our lives in many different ways. They are used, for example, to communicate with each other, shop online, find information on the internet or for digital entertainment such as gaming, music or films. There are therefore many categories of online services, from simple websites to app-stores and online platforms.

* 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.

Anyone who handles personal data outside of the personal and family sphere must comply with the General Data Protection Regulation (GDPR)[1]. Providing information on a hotline to the wrong person can be a data protection offence, as can storing customer data for too long or providing information about data that a company stores about a person too late. These processes are regulated by the GDPR, as they involve the processing of personal data that is collected and stored in analogue or digital form from individuals. However, not all data is collected from individuals. Data processing also takes place when companies collect data on computers, mobile phones, etc. via software, operating systems or browsers. Without such access by the provider of a website or app to the device from which the page is accessed, the devices cannot communicate with the provider's servers.

However, they must do so in order for data transmission to take place, which results in content being transferred from the provider's server to the end device as images, text or sound. In the European Union (EU), this type of data processing is not regulated by the GDPR, but more recently by the new Digital Services Act (DSA).[2]

2. The Aim of the Digital Services Act

In future, the DSA will regulate the activities of digital service providers within the EU. This creates one of the most important sets of digital policy regulations in Europe. Together with the Digital Markets Act (DMA)[3] , the sibling of the DSA, the new regulations are intended to become a kind of basic law for the internet. The main aim is to restrict previously uncontrolled data processing in the area of E-Commerce.

The DSA has been officially in force in the EU since 16 November 2022. In an initial phase, the DSA was only mandatory for very large online platforms and very large online search engines. The regulations have been fully applicable since 17 February 2024. It aims to protect European consumers and their fundamental rights in the digital space and ensure a level playing field for companies. Together with the DMA, the DSA is intended to form an overarching guideline for the internet. In the coming months and years, digital

[1] Regulation (EU) 2016/679 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 and on the Free Movement of such Data and Repealing Directive 95/46/EC, OJ 2016 L 119, 1.

[2] 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, OJ 2022 L 277, 1.

[3] 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, OJ 2022 L 265, 1.

providers will therefore be faced with substantial changes. The *European Council*, together with the *European Parliament*, has adopted the DSA to strengthen the digital single market.

The DSA strengthens consumer protection in the digital space through clear rules and transparency obligations. This includes imposing clear obligations on online platforms and social media. In particular, the DSA regulates the handling of illegal content and products that are brought into circulation in violation of data protection regulations. The DSA also promotes the creation of a secure and transparent digital environment. The provisions also include measures to protect freedom of expression by setting clear guidelines for the moderation of content. Providers of so-called intermediary services - for example hosting services, online marketplaces, social networks, etc. - are required by the DSA to ensure transparency. They are obliged by the DSA to be completely transparent and responsible. This will create a standardised legal framework for digital services in the EU.

3. Not a European Directive, but a European Regulation

The DSA has been directly applicable in all EU Member States since 17 February 2024, without the need for further national implementation by them. In legal terms, it is a European regulation and not just a directive.

European directives are limited to prescribing a certain result for EU Member States. However, they leave the achievement of this result to the Member States themselves; they must implement directives within certain deadlines through their own national legislation. In contrast, EU regulations are directly and immediately binding for all EU Member States and not, like a directive, only with regard to the result to be achieved.

What prompted the EU to adopt the DSA as a regulation?

With the previous data protection law, all EU Member States had the same legal basis. However, they were able to determine the implementation of data protection themselves. As a result, there was a considerable imbalance in the level of data protection in the individual EU Member States. The introduction of the DSA, which is directly and immediately binding for all Member States, was intended to eliminate this imbalance.

4. The Regulations of the DSA in Detail

The following pages present the main regulatory content of the DSA:

4.1. Material Scope of Application: "Digital Services"

The range of services covered by the DSA is immense, from online marketplaces to social networks and search engines.

The provisions of the DSA apply in principle to all "digital services". "Digital services" are generally information society services, i.e. all services that are generally provided electronically for a fee at a distance and at the individual request of recipients.[4] The DSA emphasises "intermediary services" under Article 2 (1) and includes the following services:

- "hosting" - service consisting of storing information provided by a user on their behalf[5]
- "caching" - service that consists of transmitting information provided by a user in a communication network, whereby this information is automatically cached for a limited period of time[6].
- pure "transmission" - service consisting of transferring information provided by a user to a communications network or providing access to a communications network.[7]

The specifics of the individual services are to be taken into account through a tiered regulatory system depending on their role, size and impact in the online environment: At the lowest level, there are regulations for all providers of intermediary services.[8] At the further levels, additional regulations apply cumulatively to "hosting" service providers[9] , "online platforms"[10] and "very large online platforms"[11] The former are exempted from all platform-specific obligations, meaning that they only have to comply with the

[4] See Art. 1 (1) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of the Rules of Information Society Services, OJ 2015 L 241, 1.
[5] Art. 6 of the "DSA".
[6] Art. 5 of the "DSA".
[7] Art. 4 of the "DSA".
[8] See Art. 11 et seq. of the "DSA".
[9] Art. 16 et seq. of the "DSA".
[10] See Art. 19 et seq. of the "DSA".
[11] Art. 33 et seq. of the "DSA".

obligations that are usual for all providers. However, these obligations already include some that are specifically tailored to artificial intelligence.[12]

Comprehensive obligations also apply to „very large online platforms", a term that Article 33 (1) of the DSA defines as 45 million users in the EU, whereby the *European Commission* is to be able to adjust this figure to population trends by means of a delegated act in accordance with Article 33 (2) of the DSA so that it covers around 10 percent of the EU population. The "very large online platforms" must carry out annual risk analyses[13], undergo independent audits[14] and appoint a compliance officer.[15]

The DSA replaces parts of the European E-Commerce Directive from 2000[16], but goes beyond this in regulating online platforms and imposes a degree of "social responsibility" for their business model on them.[17]

4.2. Which Providers of Digital Intermediary Services are in Focus?

The DSA applies in principle to all providers of digital services. The size is generally irrelevant, as both small and large companies are affected. However, the scope of the regulations and due diligence obligations to be followed differs in relation to the type and size of the service. This applies regardless of whether they are based in the EU or outside the EU. However, the intermediary services concerned must have a "substantial connection" to the EU. This may be the case, for example, if the service provider is established in the EU. In principle, the addressees of the DSA include cloud services, internet providers, "hosting"- service providers, online marketplaces, web shops, messenger services and social networks. To date, 19 large online services are covered by the DSA. According to the *European Commission*, the "very large online platforms" include in particular:

- Alibaba Aliexpress
- Amazon Store
- Apple AppStore

[12] For more information see *von Lewinski K., Rüpke G., Eckhardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, 2022, 256.
[13] Art. 34 et seq. of the "DSA".
[14] See Art. 37 of the "DSA".
[15] Art. 41 of the "DSA".
[16] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, OJ 2000 L 178, 1.
[17] On this see *Beck W.*, Der Entwurf des Digital Services Act - Hintergrund, Ziele und Grundsätze künftiger Regulierung des virtuellen Raums in der EU, Deutsches Verwaltungsblatt (DVBl) 2021, 1000; *von Lewinski K., Rüpke G., Eckhardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, 2022, 256.

- Booking.com
- Bing
- Google Maps
- Google Play
- Google Shopping
- Instagram
- LinkedIn
- Meta (Facebook)
- Temu
- TikTok
- Wikipedia
- X (Twitter)
- YouTube and
- Zalando.

A large number of these platforms not only exert a major influence on the opinion-forming and purchasing behaviour of users via news feeds, advertising measures and online shops, but are also at risk of using personal data in an uncontrolled manner.

4.3. The Instruments of the DSA for Enforcing the Law

The DSA has established a two-tier structure for law enforcement:[18]

4.3.1. Complaints Management and User Protection

The DSA gives users specific rights to defend themselves - for example, against breaches of data protection law.

If illegal content or breaches of data protection law are reported, online platforms must examine these reports carefully. They must provide a complaints procedure.[19] This must be easily accessible to users. Users have the right to a transparent redress procedure. For example, decisions by online platforms to delete or not to delete content or when users are denied access to a platform can be challenged. In future, providers will have to explain

[18] On this see *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].
[19] See Art. 20, 53 of the "DSA".

openly and comprehensibly how they came to their respective decision and users will be able to have this decision-making process reviewed by means of legal remedies.[20]

E-Commerce and online advertising are particularly affected by the DSA. For example, targeted advertising for minors is prohibited. Likewise, adverts may not target religion or sexual orientation. All adverts must also be labelled as such. It must also be possible to identify who has paid for the advert in question; these transparency regulations also simplify cooperation between the platforms and law enforcement authorities. In short, online platforms must clearly disclose a) that the adverts on their website are advertisements, b) who placed them and c) what factors were decisive for a user to see this particular advert.[21] Intermediary services must also set up a central contact point for electronic communication.[22]

4.3.2. Enforcement by National Supervisory Authorities

The DSA obliges the EU Member States to designate bodies for official law enforcement that independently take action against provider violations - especially in the area of data protection law - and sanction them. Only the monitoring of “very large online platforms" is carried out by the *European Commission* itself.[23]

Because the DSA protects different legal interests, several authorities may be responsible as “DSA-coordinators" in the EU Member States.[24] This also includes the data protection authorities. However, the responsibility of the authorities must be clearly regulated; it must be ruled out that user complaints are lost in a „ping-pong of authorities". [25]

The central complaints and coordination centre in Germany is the so-called *Bundesnetzagentur*. It is the point of contact during the entire period of a complaint procedure. In Germany, however, supervision is also exercised by the so-called *Bundeszentrale für Kinder- und Jugendmedienschutz*. Consumer protection organisations are also of particular importance from a consumer

[20] Art.81 et seq. of the “DSA”.
[21] *Marx L*., Der Digital Services Act der Europäischen Kommission, AnwaltZertikat IT-und Medienrecht (AnwZert ITR), №4, 2021, margin note 2.
[22] Art. 11 et seq. of the “DSA”.
[23] *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].
[24] See Art. 3 of the “DSA”.
[25] For more information see *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].

protection perspective. These are naturally very „close to the ear" of consumers due to their counselling activities and their role as a complaints receiving body.

5. Related German Law: The „Digitale-Dienste-Gesetz"

Because the DSA is a European regulation, it is directly applicable in the Member States of the EU. Unlike a European directive, it no longer needs to be transposed into national law. Nevertheless, the DSA must of course be "flanked" by national law. The EU Member States themselves are responsible for enforcing its provisions. They must harmonise their national law accordingly. In Germany, the DSA is "flanked" by the national "Digitale-Dienste-Gesetz (DDG)" of 6 May 2024[26]. It highlights the difficulties that can arise when implementing the DSA in the EU Member States.

5.1. Supplementation of the DSA by the German DDG

The German DDG of 6 May 2024 largely supplements the DSA. In this context, it replaces existing national digital law.[27]

Of particular note are regulations on the liability of online platforms for content, on the setting of cookies and on fines for legal violations. The DDG deals with liability for "hosting", "caching" and "transmission" as so-called "fault-based liability". Regulations on this and on the liability of WLAN operators are specified in § 7 and § 8 DDG. Anyone who sets or reads cookies requires the explicit consent of the user. In this respect, an explicit "cookie opt-in regulation" is indispensable.

Finally, at the end of the law there are provisions on the fines that can be imposed for violations of the DDG. For example, there is a fine of up to 50,000 euros if the so-called imprint obligation is violated. In the case of commercial

[26] Gesetz zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinien 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20.6.2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Onlinevermittlungsdiensten und zur Änderung weiterer Gesetze vom 6.5.2024 (Digitale-Dienste-Gesetz), Federal Law Gazette 2024 I, 1.

[27] *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.

communication, especially if correct sender information is concealed or hidden, the fine can even be up to 300,000 euros.

5.2. The so-called Imprint Obligation

One focus of the DDG is the so-called imprint obligation. It is an obligation to identify the service provider.[28] The so-called imprint obligation is regulated in § 5 DDG and applies to commercial digital services that are generally offered for a fee. § 5 DDG not only covers paid services, but can also apply to free services. The characteristic of payment only requires a commercial purpose of the offer.[29]

Against this background, influencer websites are also included if they advertise products or services. This does not only include monetary income that a company pays the influencer for displaying adverts. It also includes income in kind, for example if an influencer is provided with the advertised products or services free of charge by a company and is allowed to keep them.[30]

With regard to their obligation under § 5 DDG to identify the service provider, website operators must provide an imprint. The imprint must include the following informations:

- the name and address at which the service provider is established,
- in the case of legal entities, the legal form, the authorised representative, any share capital or share capital including contributions, and
- contact details, i.e. e-mail, telephone and, if applicable, fax number.

In addition, service providers may have to provide further information, such as the competent regulatory or supervisory authority, the commercial register, professional regulations and how these regulations can be accessed, as well as the tax number.

Finally, it is a requirement that the legal notice on the website is accessible via a maximum of two clicks.

[28] For more information see *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.

[29] See *Oberlandesgericht Hamburg*, decision of 3 April 2007 - 3 W 64/07, margin note 7; *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.

[30] On this see *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.

6. Conclusion

The coming years will show whether the DSA can fulfil its promises - including in terms of data protection law. The evaluation will take place by the beginning of 2027. The success of the DSA will largely depend on how well the EU Member States clarify the remaining details: They are responsible for large parts of the supervision.

Whether the DSA (together with its sibling, the DMA) has actually triggered a revolutionary development in the area of digital services,[31] will largely depend on the design of the enforcement and sanction regime, which in principle remains the preserve of the EU Member States.[32] Due to the country of origin principle, the jurisdiction of the supervisory authority is based on the location of the main establishment of the intermediary service concerned. In the context of the GDPR, for example, this decentralised principle is criticised by many experts because different national authorities sometimes act with varying degrees of speed and consistency.

In substance, however, the DSA was long overdue. After all, as technology develops, online platforms will increasingly gain market power and weaken data protection, competition and consumer protection.

Bibliography:

1. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (DSA) and amending Directive 2000/31/EC, OJ 2022 L 277.
2. 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 (DMA) and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ 2022 L 265.
3. Regulation (EU) 2016/679 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 and on the Free Movement of such Data and repealing Directive 95/46/EC (GDPR), OJ 2016 L 119.
4. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a Procedure for the Provision of

[31] The *Economist* of 15.12.2020, <https://www.economist.com/business/2020/12/15/the -eu-unveils-its-plan-to-rein-in-big-tech.html> [15.11.2024].
[32] See Recital No. 79 of the "DSA".

Information in the field of Technical Regulations and of the Rules of Information Society Services, OJ 2015 L 241.
5. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market (E-Commerce Directive), OJ 2000 L 178.
6. *Verbraucherzentrale*, Digitale Dienste: Was regelt der Digital Services Act? <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste.pdf> [15.11.2024].
7. *Beck W.*, Der Entwurf des Digital Services Act – Hintergrund, Ziele und Grundsätze künftiger Regulierung des virtuellen Raums in der EU, Deutsches Verwaltungsblatt (DVBl), 2021, 1000.
8. *Brauneck J.,* Das Verantwortungsbewusstsein der Plattformbetreiber im Digital Services Act, Neue Zeitschrift für Verwaltungsrecht (NVwZ), 2024, 377.
9. *Brorsen H., Falk R.*, Neue Compliance-Pflichten nach dem Digital Services Act, Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR), 2024, 32.
10. *Buchheim J., Schrenk M.*, Der Vollzug des Digital Services Act, Neue Zeitschrift für Verwaltungsrecht (NVwZ), 2024, 1.
11. *Legner S.*, Der Digital Services Act – Ein neuer Grundstein der Digitalregulierung, Zeitschrift für Urheber- und Medienrecht (ZUM), 2024, 99.
12. *Lorenz B.*, Die Anbieterkennzeichnung nach dem DDG, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №14, 2024, margin note 3.
13. *Marx L.*, Der Digital Services Act der Europäischen Kommission, AnwaltZertifikat IT- und Medienrecht (AnwZert ITR), №4, 2021, margin note 2.
14. *von Lewinski K., Rüpke G., Eckhardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, 2022.

Thomas Hoeren [*]
Philip Mayer [**]
Gesa Schenke [***]

"Poena Sine Culpa" in Data Protection Law? On The Validity and Scope of the Principle of Culpability in the Imposition

In the preliminary ruling proceedings in the Deutsche Wohnen case from 2023, the ECJ clarified that the supervisory authorities must be able to prove fault towards the controller when imposing fines in accordance with Art. 83 GDPR.[1] *Depending on how the decision is read, the Court thus rejected the calls for strict liability.*[2] *Meanwhile, the Berlin Court of Appeal, which referred the case to the ECJ, took note of the decision and referred it back to the competent Berlin Regional Court by order of 22 January 2024, which must reassess the legality of the fine in light of the Court's requirements.*[3] *The decision of the Court of Appeal gives cause to recapitulate the principles established by the ECJ and - as will be shown - to apply a different reasoning than that chosen by the Court of Justice. The ECJ derived the culpability requirement from a methodologically correct interpretation of Art. 83 GDPR and the general system and objective of the General Data Protection Regulation (GDPR) and thus from secondary law. The following article examines whether the culpability requirement does not already follow from*

[*] Professor, Doctor in Law, Director of the Institute for Information, Telecommunications and Media Law at the University of Münster.
[**] Research Assistant and Doctoral Candidate at the University of Münster.
[***] Research Assistant at an International Commercial Law Firm.
[1] ECJ NJW 2024, 343 para. 68.
[2] *Brink S., Wybitul T.,* ZD 2024, 137 (142); *Korte K.,* ZD-Aktuell 2024, 01500, <https://www.lto.de/recht/hintergruende/h/eugh-c80721-deutsche-wohnen-dsgvo-bussgeld-erfolg-datenschutz-beauftragte-kartellrecht> [1.03.2024].
[3] KG Berlin BeckRS 2024, 2154; see on the question referred KG Berlin ZD 2022, 156.

primary law, which is superior in terms of normative hierarchy, insofar as fines under the GDPR are criminal sanctions within the meaning of primary law. In the course of this, the article will deal with the anchoring of the principle of fault in EU law and the case law of the ECtHR on the principle of nulla poena sine culpa.

Keywords: GDPR, Deutsche Wohnen case, ECJ, Supervisory authorities, Administrative fines, Nulla poena sine culpa, European Charter of Fundamental Rights (CFR), Presumption of innocence, European Convention on Human Rights (ECHR).

1. The Principle of Fault in European Primary Law

According to the principle *of nulla poena sine culpa*, the existence of guilt is required for the imposition of punishment.[4] Guilt in the sense of personal reproachability due to intentional or negligent behaviour therefore has the function of justifying punishment and acts as a basis for legitimising the imposition of a criminal penalty (so-called guilt to justify punishment).[5] At the same time, guilt has a penalty-limiting function, which consists of the fact that the penalty may not exceed the established level of guilt (so-called penalty assessment guilt).[6] The function of guilt in justifying and limiting punishment form the core elements of the so-called guilt principle.[7] The linking of guilt to the controllable actions of the individual expresses the state's respect for the human dignity of the individual, who otherwise threatens to become a mere

[4] BVerfGE 95, 96, 131 = NJW 1997, 929 (930); BVerfGE 123, 267, 413 = NJW 2009, 2267 (2289); *Sieber U., Satzger H., von Heintschel-Heinegg F., Esser R.,* Europäisches Strafrecht, 2nd ed. 2014, § 55 para. 60. *Schönke A., Schröder H., Eisele J*., StGB, 30th ed. 2019, Vor. §§ 13 ff. para. 103; *Adam T., Schmidt F., Schumacher L.,* NStZ 2017, 7.

[5] BVerfGE 109, 133, 174 = NJW 2004, 739 (746); BVerfGE 128, 326, 376 = NJW 2011, 1931 (1938); *Roxin C., Greco L.,* Strafrecht AT I, 2020, § 19 para. 54.

[6] BVerfGE 95, 96, 140 = NJW 1997, 929 (932); *Sieber U., Satzger H., von Heintschel-Heinegg F., Esser R.,* Europäisches Strafrecht, 2nd ed. 2014, § 55 para. 60; *Roxin C., Greco L*., Strafrecht AT I, 2020, § 19 para. 9, 62.

[7] Cf. *Keil G.,* Willensfreiheit, 2nd ed. 2013, 157; *Globke*, in: *Brunhöber W., Höffler B., Kaspar F., Reinbacher R., Vormbaum M.* (eds.), Strafrecht und Verfassung, 2012, 67; *Engelhart H*., NZWiSt 2015, 201 (203); similarly *Satzger H*., ZRP 2010, 137 (139).; *Hörnle J.,* JZ 1999, 1080 (1088), is critical of the differentiation between criminal liability and criminal justification liability.

object of state arbitrariness.[8] For this reason, the Federal Constitutional Court locates the constitutional basis of the principle of guilt in the guarantee of human dignity in Article 1(1) of the Basic Law, the general freedom of action in Article 2(1) of the Basic Law and in the principle of the rule of law (Article 20(3) of the Basic Law), which, as part of the "unavailable constitutional identity"[9] of Article 79(3) of the Basic Law, marks a limit to the Europeanisation of criminal law.[10] In Union constitutional law, the dogmatic basis, content and scope of the principle of guilt are comparatively less clear.[11] The principle of *nulla poena sine culpa* is not affirmed either in the European Convention on Human Rights (ECHR) or in the European Charter of Fundamental Rights (CFR), although its recognition as a general principle of human rights is undisputed.[12] The European Court of Justice only implicitly takes the principle of guilt into account when reviewing criminal sanctions as part of the general proportionality test.[13] In contrast, the European Commission, the Council and the European Parliament have explicitly recognised the principle of guilt.[14] Advocate General Kokott also sees the principle *of nulla poena sine culpa* "implicitly contained both in Article 48(1) of the [Charter of Fundamental Rights] and in Article 6(2) of the ECHR" and both provisions "as procedural manifestations of the principle of nulla poena sine culpa."[15] Other This assumption will be analysed below.

1.1. Guarantee of Human Dignity, Art. 1 CFR

The case law of the Federal Constitutional Court on the principle of guilt suggests that the principle of guilt should be anchored in primary law in the

[8] BVerfGE 30, 1, 41 = NJW 1971, 275 (282); on the object formula *Scholz* R., *Dürig* G., *Herzog* R., *Herdegen* M., GG (Vol. I), Art. 1 para. 36.
[9] BVerfGE 123, 267, 344 = NJW 2009, 2267 (2270).
[10] BVerfGE 123, 267, 348 = NJW 2009, 2267 (2271); see *Adam T., Schmidt F.*, *Schumacher L.*, NStZ 2017, 7 (8).
[11] *Böse M., Stuckenberg C.*, Europäisches Strafrecht (EnzEuR Bd. 11), 2nd ed. 2021, § 10 para. 17; *Globke* R., in: *Brunhöber B.*, *Höffler H., Kaspar J., Reinbacher T., Vormbaum M.* (eds.), Strafrecht und Verfassung, 2012, 66 f.; *Vogel J.*, JZ 1995, 331 (337).
[12] *Grabitz E., Hilf M., Nettesheim M., Vogel P., Eisele J., Das Recht der Europäischen Union, 80th ed. 2023, Art. 83 TFEU, para. 46; Sieber U., Satzger H., von Heintschel-Heinegg F., Killmann A.,* Europäisches Strafrecht, 2nd ed. 2014, § 11 para. 18; *Hochmayr G.,* ZIS 2016, 226 (230); *Fromm E.*, ZIS 2007, 279 (287); *Tiedemann K.,* NJW 1993, 23 (28).
[13] ECJ judgement of. 16.11.1983, Case 188/82, ECR 1983, 3721 para. 18 - *Thyssen*; ECJ judgement of 18.11.1987, Case 137/85, ECR 1987, 4587 para. 14 - *Maizena*; ECJ judgement of 11 July 2002, Case C-210/00, ECR 2002 I-6453 para. 44 - *Käserei Champignon Hofmeister*.
[14] See COM(2011) 573 final, 10; Council Doc. 16542/2/09 REV 2 No. 6-8; European Parliament resolution of 22 May 2012 on the EU approach to criminal law (2010/2310(INI)), C 264 E/9.
[15] Opinion GA Juliane Kokott, 28 February 2013, Case C-681/11, EU:C:2013:126, para. 41; see also Opinion GA Carl Otto Lenz, 11 July 1992, Case C-143/91, EU:C:1990:381.

guarantee of human dignity in Art. 1 CFR. Under constitutional law, Art. 1 CFR guarantees the right of every person to social value and respect, which is due to them solely because of their humanity and regardless of their characteristics, performance or social status.[16] Accordingly, all state measures that undermine the quality of the human being as a subject are significant interference and incompatible with human dignity.[17] In criminal and quasi-criminal proceedings, a conflict with the human dignity of the accused arises in any case if the actions of the accused are disapproved of by the state in terms of social ethics and are accused of injustice.[18] In contrast, the mere determination of guilt and measures serving to establish guilt do not conflict with human dignity.[19] A closer look at the case law of the Federal Constitutional Court also reveals that the principle of guilt is regularly derived from the triad of Article 1 (1) of the Basic Law, the principle of the rule of law and Article 2 (1) of the Basic Law and not solely from the guarantee of human dignity.[20] The principle of guilt is therefore - at least directly - not anchored in the guarantee of human dignity in Article 1 of the Basic Law. [21]

1.2. Presumption of Innocence, Art. 48 para. 1 CFR, Art. 6 para. 2 ECHR

Art. 48 para. 1 CFR is part of the catalogue of procedural guarantees under criminal law and corresponds almost entirely to Art. 6 para. 2 ECHR.[22] Both provisions standardise the so-called presumption of innocence, according to which, in criminal or quasi-criminal proceedings, the innocence of every accused or defendant is presumed until guilt is proven in accordance with the law.[23] The presumption of innocence does not only apply to EU citizens and natural persons, as evidenced by the wording "any accused person" and "any

[16] *Jarass H. D.,* GRC, 4th ed. 2021, Art. 1 GRC para. 6, 7.
[17] *Jarass H. D.,* GRC, 4th ed. 2021, Art. 1 GRC para. 8.
[18] *Globke* R., in: *Brunhöber* B., *Höffler* K., *Kaspar* J., *Reinbacher* T., *Vormbaum* M. (eds.), Strafrecht und Verfassung, 2012, 59; *Frister* H., Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1988, 25.
[19] *Rabe P.,* Das Verständigungsurteil des Bundesverfassungsgerichts und die Notwendigkeit von Reformen im Strafprozess, 2017, 147; *Frister H*., Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1988, 25.
[20] The so-called Lisbon judgement BVerfGE 123, 267, 413 = NJW 2009, 2267 (2289) is an exception.
[21] See *Schaut A. B*., Europäische Strafrechtsprinzipien, 2012, 228; *Vogel P*., JZ 1995, 331 (339); See also *Böse M., Satzger H.,* Europäisches Strafrecht (EnzEuR Bd. 9), 1st ed. 2013, § 2 para. 59.
[22] Explanations on the Charter of Fundamental Rights, OJ 2007 No. C 303/17, 30.
[23] *Calliess C., Ruffert M., Blanke H., EUV/AEUV, 6th ed. 2022, Art. 48 CFR para. 1, 4; Meyer J., Hölscheidt S., Eser A., Kubiciel M., CFR, 5th ed. 2019, Art. 48 CFR para. 1.*

person", but is a human right that can also be invoked by legal persons.[24] According to Article 51(1) of the CFR, all institutions, bodies, offices and agencies of the Union are bound by it when implementing Union law, including in particular courts, prosecuting authorities and investigating authorities.[25] In criminal proceedings and proceedings of a quasi-criminal nature, the presumption of innocence therefore manifests itself in the prohibition of a guilty verdict and the imposition of penalties and sanctions without (prior) legal proof of guilt.[26] The prohibition of suspicion-based punishment derived from the presumption of innocence can therefore be understood as a procedural expression of the principle of guilt, as it expresses the function of guilt as a core element of the principle of guilt to justify punishment.[27] The principle of guilt is therefore implicitly anchored in the presumption of innocence in Art. 48 para. 1 CFR and Art. 6 para. 2 ECHR.[28]

1.3. Principle of Proportionality, Art. 49 para. 3 CFR

Art. 49 para. 3 CFR standardises the principle of proportionality under EU law for criminal offences and administrative sanctions and ensures that penalties and quasi-criminal sanctions imposed by courts and authorities must be proportionate in each individual case.[29] In other words, penalties and sanctions must be appropriate, necessary and proportionate. A penalty imposed does not meet the criterion of proportionality in particular if the penalty is not proportionate to the wrongfulness and culpability of the offence, whereby the severity of the offence and the weight of the penalty must be taken into account.[30] The principle of proportionality of guilt and punishment,

[24] *Calliess C., Ruffert M., Blanke H., EUV/AEUV, 6th ed. 2022, Art. 48 CFR para. 2; Jarass H. D., CFR, 4th ed. 2021, Art. 48 para. 12.*

[25] *Meyer J., Hölscheidt S., Eser A., Kubiciel M.,* GRC, 5th ed. 2019, Art. 48 GRC para. 13; *Calliess* C., *Ruffert* M., *Blanke* H., EUV/AEUV, 6th ed. 2022, Art. 48 GRC para. 4..

[26] *Meyer J., Hölscheidt S., Eser A., Kubiciel M.*, GRC, 5th ed. 2019, Art. 48 GRC para. 6, 7; *Calliess* C., *Ruffert* M., *Blanke* H., EUV/AEUV, 6th ed. 2022, Art. 48 GRC para. 4.

[27] *Meyer J., Hölscheidt S., Eser A., Kubiciel M*., GRC, 5th ed. 2019, Art. 48 GRC para. 10.

[28] Cf. *Frister H.,* Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1988, 89; *Engels H.,* , Unternehmensvorsatz und Unternehmensfahrlässigkeit im Europäischen Kartellrecht, 2002, 71; *Böse M., Satzger C.,* Europäisches Strafrecht (EnzEuR vol. 9), 1st ed. 2013, § 2 para. 59; differentiated *Klaas A., Momsen C., Wybitul T*., 71; *Böse M., Satzger C.,* Europäisches Strafrecht (EnzEuR Bd. 9), 1st ed. 2013, § 2 para. 59; differentiated *Klaas A., Momsen C., Wybitul T., Cornelius K., Datenschutzsanktionenrecht*, 1st ed. 2023, § 2 para. 22.

[29] *Jarass H.D.,* GRC, 4th ed. 2021, Art. 49 GRC para. 17; *Pechstein M., Nowak R., Häde U., Schröder R.*, Frankfurter Kommentar EUV/AEUV/GRC, 2nd ed. 2023, Art. 49 para. 20.

[30] *Jarass H.D.,* GRC, 4th ed. 2021, Art. 49 GRC para. 19; *Pechstein M., Nowak R., Häde U., Schröder R.,* Frankfurter Kommentar EUV/AEUV/GRC, 2nd ed. 2023, Art. 49 para. 20.

which is expressed in Article 49(3) of the CFR, therefore has a penalty-limiting function.[31] The penalty-limiting function of guilt is also a core element of the principle of guilt. In this respect, the principle of guilt is also implicit in the principle of proportionality in Art. 49 para. 3 CFR. [32]

1.4. Interim Result

In conclusion, it should be noted that the principle of guilt is enshrined in primary law both in the presumption of innocence in Art. 48 para. 1 CFR and Art. 6 para. 2 ECHR as well as in the principle of proportionality in Art. 49 para. 3 CFR.

2. Derivation of the Culpability Requirement in the "Deutsche Wohnen Judgement"

In the preliminary ruling procedure, the ECJ had to deal with the question of whether Art. 83 GDPR requires proof of culpability in the sense of an intentional or negligent breach of Art. 83 (4) - (6) GDPR for the imposition of fines on the controller as a legal person.[33] With regard to the second question referred, the Court of Justice first states that Art. 83 GDPR does not expressly require a negligent or culpable breach for the imposition of fines. Instead, the ECJ refers to the wording of Art. 83 para. 2 sentence 2 lit. b) GDPR, according to which the intentional or negligent nature of an infringement must be duly taken into account when deciding on the imposition of a fine.[34] None of the other criteria mentioned in Art. 83 para. 2 sentence 2 GDPR suggest that the controller is liable regardless of fault.[35] Rather, Article 83(3) GDPR also speaks against strict liability, according to which a culpable breach by the controller is also required.[36] The result resulting from the wording of Art. 83 GDPR is confirmed by the purpose and the general system of the GDPR, which grants the supervisory authorities a margin of discretion with regard to the imposition

[31] *Meyer J., Hölscheidt S., Eser A., Kubiciel M.,* GRC, 5th ed. 2019, Art. 49 GRC para. 38.
[32] *Klaas A., Momsen C., Wybitul T., Cornelius K.,* Datenschutzsanktionenrecht, 1st ed. 2023, § 2 para. 36; Kaufmann, JURA 1986, 225 (227); *Schaut A.*, Europäische Strafrechtsprinzipien, 2012, 228.
[33] ECJ, NJW 2024, 343 para. 61.
[34] ECJ, NJW 2024, 343 para. 62.
[35] ECJ, NJW 2024, 343 para. 66.
[36] ECJ, NJW 2024, 343 para. 67.

of fines and other remedial measures with the provision of Art. 58 para. 2 lit. i) GDPR and thus provides a differentiated system of sanctions.[37] The Union legislator has deliberately dispensed with the possibility of imposing fines regardless of fault.[38] As a result, in the view of the Court of Justice, both the wording of Art. 83 GDPR and the system and purpose of the GDPR speak in favour of the requirement of a culpable breach of the obligations set out in Art. 83 (4) - (6) GDPR for the imposition of fines.

3. GDPR Fines as Part of Criminal Law?

Although the European Court of Justice refrained from categorising the GDPR fines in the system of sanctions under EU law, it still considers proof of fault to be necessary when issuing fines under the GDPR and is therefore unspokenly committed to the validity of the principle of fault. This is unspoken because it does not cite considerations of Union constitutional law to justify the culpability requirement, but instead endeavours to interpret secondary law. However, the question arises as to whether this result does not already follow from EU constitutional law, insofar as the GDPR fines, by their legal nature, prove to be criminal law in at least a broader sense.[39] To this end, the requirements for the existence of criminal law sanctions in general are developed below in order to then apply the criteria to data protection sanctions law in concrete terms.

3.1. Engel Criteria

According to established case law of the ECJ, three criteria are decisive in assessing the legal nature of the prosecution measures and sanctions in question: firstly, the legal classification of the offence under national or supranational law, secondly, the nature of the offence and thirdly, the severity of the sanction threatening the person concerned.[40] To this end, the ECJ has adopted the Engel case law of the ECtHR, which defined the concept of

[37] ECJ, NJW 2024, 343 para. 70, 73.
[38] ECJ, NJW 2024, 343 para. 74.
[39] Similarly*, Hochmayr G.*, ZIS 2016, 226.
[40] ECJ, BeckRS 2012, 81043 para. 37 - Bonda; ECJ, BeckRS 2018, 6055 para. 26 f. - Menci Luca; ECJ, BeckRS 2022, 5011 para. 25 - bpost; *Gassner K., Seith S.,* Ordnungswidrigkeitengesetz, 2nd ed. 2020, Introduction para. 6.

criminal proceedings.[41] The factors known in the literature as the *Engel criteria* are initially independent of each other and thus open up alternative access to the criminal law guarantees such as the principle of guilt.[42]

a) The will of the Legislator

According to the first criterion, the intention of the (supra-)national legislator must first be taken into account and the question asked as to whether it categorises the proceedings and measures in question as administrative or criminal law proceedings and measures.[43] The national judgement is a sufficient but not a necessary condition.[44] Otherwise, the categorisation would depend on the free decision of the member states or contracting states.[45]

b) The Nature of the Offence

Secondly, the type of offence, i.e. the nature of the offence, must be used to determine whether the sanction imposed pursues a repressive objective.[46] According to this, it is the nature of criminal sanctions to pursue both preventive and repressive purposes.[47] The material and personal scope of application of the norm is particularly important on the factual side; especially if it is (potentially) directed at the general public, this speaks in favour of the criminal nature of the offence.[48] The protection of particularly important community interests can also be used in favour of a criminal sanction.[49]

[41] ECtHR, EuGRZ 1976, 221 - Engel et al. v Netherlands; ECtHR, BeckRS 2010, 21072 para. 53 - Zolotoukhine v Russia; ECJ, NJW 2024, 33, para. 45 - Volkswagen Italia SpA; *Grabenwarter C., Pabel K.*, ECHR, 6th ed. 2016, § 24 para. 19; critical *Wegner*, NZWiSt 2023, 401.
[42] A cumulative application of the second and third criteria is only necessary if the consideration of individual criteria does not produce a clear result; *Meyer-Ladewig J., Nettesheim M., von Raumer S., Harrendorf H., König P., Voigt T.,* ECHR, 5th ed. 2023, ECHR Art. 6 para. 23.
[43] ECJ, BeckRS 2023, 8994 para. 40.
[44] ECJ, BeckRS 2022, 5011 para. 26; *Karpenstein U., Mayer F.C.,* ECHR, 3rd ed. 2022, Art. 6 para. 25.
[45] *Barrot W.,* ZJS 2010, 701, 702; *Gerhold S.*, 41st ed., Introduction to the OWiG para. 5.
[46] ECJ, BeckRS 2018, 6055 para. 31.
[47] ECJ, BeckRS 2023, 8994 para. 42; ECJ, BeckRS 2023, 24054 para. 49; *Grabenwarter C., Pabel K.*, ECHR, 6th ed. 2016, § 24 para. 21.
[48] *Dörr C., Grote H., Marauhn T.,* ECHR/GG, 3rd ed. 2022, ch. 14 para. 26; *Grabenwarter C., Pabel K.,* ECHR, 6th ed. 2016, § 24 para. 21.
[49] *Karpenstein U., Mayer F.C.,* ECHR, 3rd ed. 2022, Art. 6 para. 26.

c) The Severity of the Sanction

Thirdly, with regard to the severity of the sanctions, a distinction must be made between fines and custodial sentences. While custodial sentences are generally of a criminal nature, fines and other measures restricting freedom must be assessed on a case-by-case basis according to the severity of the consequences.[50] The degree of severity is determined in particular by the maximum penalty provided for in the regulations, which must be of a not entirely insignificant weight in order to represent a serious consequence for the person concerned.[51]

3.2. Art. 58 para. 2 lit. i), 83 para. 4-6 GDPR in the Light of the Engel Criteria

Against the background of the culpability requirement stipulated in the *Deutsche* Wohnen *decision*, the following examines whether - applying the Engel criteria just described - the offence of imposing a fine under Art. 83 GDPR is criminal law in (at least) the broader sense and whether the culpability requirement therefore already follows from the principle of culpability under EU law.[52]

a) The will of the legislator

With the above in mind, the first Engel criterion must first be applied in such a way that the will of the supranational legislator in Brussels itself must be investigated as to what legal nature it assigns to data protection fines.[53] A clear commitment to or against criminal law cannot be inferred from Art. 58 para. 2 lit. i), 83 para. 4-6 GDPR. In European antitrust law, the situation is different *de lege lata*. Art. 23(5) of the Cart Regulation makes it clear that the fines imposed on companies pursuant to Art. 23(1) and (2) of the Cart Regulation in the event of infringements of antitrust provisions are not of a criminal nature.[54] In legislative practice, the antitrust fines act as a blueprint

[50] ECtHR, BeckRS 2010, 2107253 - Zolotoukhine v Russia; *Dörr C., Grote H., Marauhn T.*, ECHR/GG, 3rd ed. 2022, ch. 14 para. 26; *Barrot W.,* ZJS 2010, 701 (702).
[51] A sanction in the amount of EUR 500 is not sufficient in any case; ECtHR, BeckRS 2010, 21072; ECJ, BeckRS 2023, 8994 para. 46; ECJ, BeckRS 2023, 24054 para. 53; *Grabenwarter C., Pabel K.,* ECHR, 6th ed. 2016, § 24 para. 22; *Jarass H.*, GRC, 4th ed. 2021, Art. 48 GRC para. 9.
[52] ECJ, NJW 2024, 343 para. 75, 78 - Deutsche Wohnen.
[53] *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P*., ECHR, 5th ed. 2023, ECHR Art. 6 para. 24.
[54] *Bechtold R., Bosch N., Brinker I., Bechtold R.,* EU-Kartellrecht, 4th ed. 2023, Regulation (EC) 1/2003, Art. 23 para. 91.

for sanction mechanisms in other areas of law determined by EU law.[55] There are also certain overlaps between fines in antitrust law on the one hand and data protection law on the other, as can be seen explicitly in recital 150 of the GDPR. Accordingly, when fining controllers that are also companies, the functional concept of an undertaking under Art. 101, 102 TFEU must be used, at least on the legal consequences side, to determine the amount of the fine based on the amount of the previous year's total turnover.[56] In view of these obvious overlaps with fines under antitrust law, the EU legislator probably pursued an objective comparable to Art. 23(5) GDPR when adopting the GDPR and did not assign the fines under data protection law to criminal law either.

This interpretation is in line with the few indications in the GDPR regarding the legal nature of fines under data protection law. For example, Art. 84 para. 1 GDPR in conjunction with recital 149 GDPR. Recital 149 of the GDPR stipulates that Member States should impose criminal sanctions for breaches of data protection law, in particular if the offences are not already sanctioned under Art. 83 of the GDPR. The German legislator has willingly made use of this opening clause in Section 42 BDSG.[57] If the criminal sanctions under data protection law are located at this point in contrast to Art. 83 GDPR, the European legislator considers the fines under data protection law to be an aliud and therefore purely administrative sanctions.[58] Accordingly, recitals 150 and 152 of the GDPR also refer to administrative sanctions as distinct from criminal law.[59] This finding is consistent with the legislative genesis, according to which the GDPR is based solely on Art. 16 para. 2 GDPR and therefore no criminal law authorisation basis was used. In any case, such a basis has only been established in EU law in the area of financial sanctions law pursuant to Art. 325 para. 4 TFEU.[60] It can therefore be assumed overall that the European legislator merely intended to enact purely administrative sanctions with Art. 58 para. 2 lit. i), 83 GDPR.[61] According to the above, however, the first Engel criterion is merely indicative, so that the legislator is not allowed to decide for

[55] *Ackermann T.,* ZEuP 2023, 529 (555 et seq.) on the transfer of the functional concept of an undertaking under antitrust law to other areas of law; see also *Zelger F.,* EuR 2021, 478 (481 et seq.).
[56] However, the ECJ made it clear that the principle of the "functionary" under antitrust law is not relevant at the level of the substantive establishment of liability. Rather, the concept of an undertaking under antitrust law is only to be used on the legal consequences side; ECJ, NJW 2024, 343 para. 53, 57 - Deutsche Wohnen; see also LG Bonn, MMR 2021, 173 para. 30 on the use of the concept of an undertaking to establish liability.
[57] *Parigger M., Helm T., Stevens-Bartol E., Müller R.,* Labour and Social Criminal Law, 1st ed. 2021, Section 42 BDSG para. 1.
[58] See *Bülte J.*, StV 2017, 460 (461).
[59] See *Bülte J.*, StV 2017, 460 (461).
[60] *Sydow G., Marsch N., Sydow H*., DS-GVO/BDSG, 3rd ed. 2022, Introduction para. 21; cf. *Schwarze J., Becker U., Hatje A., Schoo J., Schoo M.*, EU Commentary, 4th ed. 2019, TFEU Art. 325 para. 27.
[61] See also *Bülte J*, StV 2017, 460, 461.

itself on the application of the criminal law guarantees enshrined in international and primary law, such as the principle of guilt.[62]

b) The nature of the offence

The second Engel criterion is therefore of decisive importance, according to which the nature of the offence must now be examined with regard to the GDPR fines.

aa) Addressees of the GDPR fines

The fact that the fines in data protection law are not directed at the general public, but rather as a special offence primarily against controllers and processors, speaks against a criminal sanction.[63] With regard to the narrow group of addressees, Art. 83 para. 4-6 GDPR is similar to disciplinary law, which is traditionally not categorised as criminal law according to the case law of the ECtHR.[64] In the application of the standard, however, the group of addressees under data protection law is considerably wider, as the GDPR does not impose any explicit restrictions on the personal nature of the addressee of the standard, so that in addition to any natural person processing data, legal persons can also be suitable offenders as controllers or processors (Art. 4 No. 7, 8 GDPR).[65] In this respect, data protection law differs from disciplinary law.

bb) Sanctioning of legal persons

However, this also shows a further difference to core criminal law, as legal persons are also suitable addressees of fines via the broadly understood concept of the data controller under data protection law. In criminal law in the

[62] *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P*., ECHR, 5th ed. 2023, ECHR Art. 6 para. 24.
[63] On the classification of Art. 83 para. 4-6 GDPR as a special offence *Böttger M., Zoch S.,* Wirtschaftsstrafrecht, 3rd ed. 2023, ch. 17 Data Protection Criminal Law para. 136.
[64] ECtHR, BeckRS 1976, 107962 para. 81 f.; *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P.,* ECHR, 5th ed. 2023, ECHR Art. 6 para. 25.
[65] According to Art. 4 No. 7 Hs. 1 GDPR, the controller is the "natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data"; *Simitis S., Hornung G., Spiecker i., Petri T.,* Datenschutzrecht, 1st ed. 2019, GDPR Art. 4 No. 7 para. 23; *Böttger M., Zoch S.,* Wirtschaftsstrafrecht, 3rd ed. 2023, Chapter 17 Data Protection Criminal Law para. 137.

narrower sense, only natural persons are traditionally sanctioned as legal entities, particularly in view of the history of German legislation.[66] In line with this, the Federal Constitutional Court has consistently linked the principle of guilt to human dignity in accordance with Article 1 (1) of the Basic Law, which cannot necessarily be attributed to legal persons as a legal fiction. As a result, some argue that the constitutional anchoring of the principle of *nulla poena sine culpa* precludes the introduction of corporate criminal law at national level. [67]

Nevertheless, these doubts do not apply to the criminal law categorisation of sanctions against legal persons at supranational level. It has already been emphasised that the ECJ allows the principle of guilt to be incorporated into the principle of proportionality in Art. 49 (3) CFR; this does not differentiate between natural and legal persons.[68] Accordingly, the cartel law fines set out in Article 23 (1) and (2) of the Cartel Regulation are already based on intentional or negligent behaviour on the part of the company itself.[69] Ultimately, Art. 23 para. 5 of the Cart Regulation is merely intended to clarify in this context that the European legislator - aware of its lack of legislative competence in this area - did not intend criminal offences in the original sense against natural persons.[70] The ECJ also recognises the original culpability of legal persons in its decision in the *Deutsche Wohnen* case, in which, as in antitrust law, it refers to the fault of the company itself.[71]

cc) Administrative Procedure and Opportunity Principle

However, the argument that fines are subject to the discretion of the supervisory authorities pursuant to Art. 58 (i), 83 GDPR as part of the administration, whereas criminal law judgements are generally issued by the courts, is of greater importance in the classification of fines under data protection law in the context of the second Engel criterion.[72] This has far-reaching consequences for the sanctioning procedure: The principle of legality

[66] Nevertheless, criminal law in the narrower sense against associations already exists in other countries outside of common law, as has been the legal practice in the Netherlands since 1951; *Mitsch W., Rogall K.,* KK OWiG, 5th ed. 2018, OWiG § 30 para. 258, 270.
[67] For example, *Geco*, GA 2015, 503 (504).
[68] *Sieber U., Satzger H., von Heintschel-Heinegg F., Esser R*., European Criminal Law, 2nd ed. 2014, § 55 para. 63.
[69] On culpability in European antitrust law *Schröter H., Jakob M., Klotz R., Mederer W., Kienapfel P.,* Europäisches Wettbewerbsrecht, 2nd ed. 2014, Art. 23 Kart-VO para. 39 f.
[70] In addition, the purpose of Art. 23(5) of the Cart Regulation is to ensure that the criminal law consequences of some national legal systems apply to antitrust fines; *Bechtold R., Bosch W., Brinker I.,* EU-Kartellrecht, 4th ed. 2023, Art. 23 Cart Regulation para. 91.
[71] ECJ, NJW 2024, 343, 347 para. 68, 78 - Deutsche Wohnen.
[72] *Ehmann E., Selmayr M.,* DS-GVO, 2nd ed. 2018, Art. 58 DS-GVO para. 18, 27.

applies in criminal law in the narrower sense in accordance with Section 152 (2) of the German Code of Criminal Procedure (StPO), whereas the supervisory authorities have a discretionary power and therefore the principle of opportunity applies, as confirmed by the reference in Section 41 (2) sentence 1 BDSG to Section 47 OWiG.[73] The principle of opportunity also underlies Recital 148 GDPR, according to which "in the case of a minor infringement or where the fine likely to be imposed would impose a disproportionate burden on a natural person, a warning may be issued instead of a fine".[74]

However, this does not result in any significant discrepancies between data protection sanctions law and core criminal law. The opportunity principle in data protection law must be interpreted autonomously to the effect that, as a rule, the supervisory authorities' discretion to effectively enforce Union law is reduced to zero. Only in exceptional cases is it possible to refrain from imposing fines, so that the principle of opportunity approaches the principle of legality in legal practice.[75] Furthermore, sanctions issued in administrative proceedings can also be categorised as criminal law in the broader sense. National courts only have a corresponding monopoly for criminal offences as criminal law in the narrower sense.[76]

dd) Repressive Purpose of the Fine

Finally, it depends on whether the European legislator is pursuing repressive punitive purposes with the fines under data protection law.[77] The wording of Art. 83(1) GDPR at least suggests that the sanctions regime has a preventive purpose. Accordingly, each supervisory authority shall ensure that "the imposition of fines pursuant to this Article for infringements of this Regulation [...] is effective, proportionate and dissuasive in each individual case." Above all, the last criterion of deterrence has both a special (against the addressee of the fine) and general preventive (against the general public)

[73] On the application of the opportunity principle *Böttger M., Zoch S.,* , Wirtschaftsstrafrecht, 3rd ed. 2023, ch. 17 Datenschutzstrafrecht para. 280-282; on the illegality of the reference to Section 47 OWiG in Section 47 para. 2 sentence 1 BDSG in favour of a legality principle, see *Kühling J., Buchner B., Bergt M.*, DS-GVO/BDSG, 4th ed. 2024, Section 41 BDSG para. 16; *Barthe C., Gericke J., Diemer H.*, StPO, 9th ed. 2023, Section 152 StPO para. 4.

[74] *Bülte J.*, StV 2017, 460 (463).

[75] See also *Böttger M., Zoch S.*, Wirtschaftsstrafrecht, 3rd ed. 2023, ch. 17 Data Protection Criminal Law para. 282; *Gola P.,* CR 2018, 353 (355 f.).

[76] *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P.*, ECHR, 5th ed. 2023, Art. 6 ECHR para. 23.

[77] ECJ, BeckRS 2023, 8994 para. 42; ECJ, BeckRS 2023, 24054 para. 49; BeckRS 2023, 24054 para. 49; *Grabenwarter C., Pabel K.* ECHR, § 24 para. 21.

thrust with a view to future compliance with data protection law.[78] In addition, Art. 58(2)(i), 83 GDPR should also penalise data protection violations per se in a repressive manner in order to do justice to the fundamental importance of Art. 16 TFEU and Art. 7, 8 CFR under Community law. [79]

Finally, even according to the principle of *ultra posse nemo obligatur*, which dates back to Roman law, behaviour can only be controlled by fines if the addressee can be proven to be at fault in accordance with the principle of culpability applicable in criminal law .[80] No one can be obliged to behave in an impossible manner. If the obligated party has no alternative options and is therefore not at fault, they will not deviate from their behaviour in the future. The fine therefore not only fails to have the intended steering effect; it also lacks a reason to legitimise the sanction. [81]

ee) Interim Result

Even if the last argument circularly infers the criminal nature of the GDPR fines from the necessary fault requirement, there is much to be said for interpreting the second Engel criterion in favour of the criminal nature of the sanction.

c) The Severity of the Sanction

The application of the third criterion also leads to this result: According to this criterion, the maximum amount of the fine under Art. 58 para. 2 lit. i), 83 GDPR must represent a not insignificant weight. The (potential) amount of the fines pursuant to Art. 83 (5), (6) GDPR of up to 4% of the total global annual turnover achieved in the previous financial year therefore represents a maximum sanction with considerable weight.[82] Irish *Data Protection Commission* recently imposed a fine of EUR 1.2 billion on a social network, demonstrating that this sharp sword is indeed used in practice.[83]

[78] *Parigger M., Helm T., Stevens-Bartol E., Müller R.,* Labour and Social Criminal Law, 1st ed. 2021, Art. 83 GDPR para. 92.
[79] See also recitals 148 and 152 GDPR; *Sydow G., Marsch N.*, DS-GVO/BDSG, 3rd ed. 2022, Art. 83 GDPR para. 2.
[80] *Hassemer W.,* ZRP 2011, 192, illustrates this principle, which goes back to *Publius Iuventius Celsus*.
[81] *Heckmann D.*, MMR 2023, 816 (818); in a different context on the validity of the principle of *ultra posse nemo obligatur* in data protection law *Hacker,* MMR 2018, 779 (784).
[82] *Paal B., Pauly D. A., Frenzel E.*, DS-GVO/BDSG, 3rd ed. 2021, Art. 83 DS-GVO para. 18-26; *Jarass H.*, GRC, 4th ed. 2021, Art. 48 GRC para. 9.
[83] *Klaas A., Basar B.*, ZD 2023, 477.

3.3. Result

The application of the second and third Engel criteria to the offence of fines under Art. 83 GDPR means that - contrary to the aim of the European legislator - GDPR fines are to be regarded as sanctions under criminal law in the broader sense, in line with the case law of the ECJ and ECHR. Consequently, the principle of *nulla poena sine culpa* enshrined in primary and international law applies, which means that the supervisory authorities are obliged to prove culpability to the controller when imposing fines due to the legal nature of the sanctions regime pursuant to Art. 58 (2) (i), 83 GDPR.[84]

4. Wasted Potential of the "Deutsche Wohnen Judgement"

The derivation of the culpability requirement from the assignment of data protection sanctions to criminal law is not only important from a dogmatic point of view. An understanding of criminal law means that, in addition to the principle of culpability, other guarantees of the rule of law also apply.[85] In preliminary ruling proceedings brought by the VW Group against a fine imposed by the Italian competition authority, the ECJ recently ruled that fines under unfair competition law are criminal law in the broader sense, thus confirming the validity of the *ne bis in idem* principle pursuant to Art. 50 CFR.[86] The prohibition of double jeopardy is not entirely foreign to data protection law, as Art. 84 GDPR in conjunction with recital 149 GDPR shows. Recital 149 GDPR clarifies in relation to national data protection sanctions.[87] Nevertheless, a clarification by the ECJ that this legal principle is also secured under primary law in accordance with Art. 50 CFR via the legal nature of data protection sanctions as criminal law in the broader sense would have been very welcome. The same applies to the principle of legality under Art. 49 para. 1 sentence 1 CFR in conjunction with Art. 7 para. 1 ECHR. Art. 7 para. 1 ECHR, although in connection with the GDPR's fines, compliance with the principle of certainty in

[84] Also interpreting the GDPR fines as criminal sanctions, *Drewes S., Walchner W.*, CR 2023, 163 (168); with further comments *Sydow G., Marsch N.,* DS-GVO/BDSG. 3rd ed. 2022, Art. 83 GDPR para. 3; Wolff H. A., Brink S., von *Ungern-Sternberg M. A., Holländer*, Data Protection Law, 46th edition 2021, Art. 83 GDPR para. 4.2.
[85] *Vogel*, JZ 1995, 331 (337).
[86] ECJ, NJW 2024, 33 para. 55.
[87] *Klaas A., Momsen C., Wybitul T., Klaas A.,* Datenschutzsanktionenrecht, 1st ed. 2023, § 27 para. 34.

particular has often been questioned in the literature.[88] Furthermore, the rule of law guarantees of the presumption of innocence pursuant to Art. 6 para. 2 ECHR in conjunction with Art. 48 para. 1 CFR are also relevant. Art. 48 para. 1 CFR, the right to a fair trial pursuant to Art. 6 para. 1 ECHR and, last but not least, the principle of the prohibition of self-incrimination (*nemo teneur se ipsum accusare*) in data protection sanctions law must also be observed.[89] To the extent that the ECJ derives the principle of guilt in data protection law primarily from systematic considerations and does not tie it to the classification of the sanctions regime in terms of its legal nature as criminal law in the broader sense, the Court of Justice forfeits the opportunity to clarify the foundation of data protection sanctions law under Union constitutional law and to outline the rule of law guarantees of Union constitutional law more clearly.

5. Summary

In its landmark decision in the Deutsche Wohnen case, the ECJ rightly clarifies that fines may only be imposed under the GDPR if the controller is at fault. Regrettably, Luxembourg only takes into account the system and purpose of the data protection sanction instrument. Furthermore, the application of the culpability principle is already mandatory due to the categorisation of GDPR fines as criminal sanctions. To the extent that the ECJ disregards the legal nature, it mitigates the scope of its decision with regard to the validity of the rule of law guarantees in data protection sanctions law as a whole. Nevertheless, one aspect of the ECJ judgement is beyond question: the principle of nulla poena sine culpa also applies in the GDPR.

[88] This applies all the more with the recognition of direct corporate liability; ECJ, NJW 2024, 343, 347 para. 60 - Deutsche Wohnen; *Sydow G., Marsch N.*, DS-GVO/BDSG, 3rd ed. 2022, Art. 83 DS-GVO para. 3 f.; *Gola P., Heckmann D.,* DS-GVO/BDSG, 3rd ed. 2022, Art. 83 DS-GVO para. 24.

[89] For the concretisation of the prohibition of self-incrimination in simple law, see Section 43 (4) BDSG in conjunction with Art. 33 GDPR. Art. 33 GDPR; *Klaas A., Momsen C., Wybitul T., Cornelius K.*, Datenschutzsanktionenrecht, 1st ed. 2023, § 2 Grundlagen para. 126; *Sydow G., Marsch N.* DS-GVO/BDSG, 3rd ed. 2022, Art. 83 GDPR para. 3.

Bibliography:

1. *Ackermann T.,* ZEuP 2023, 529 (555 et seq.).
2. *Adam T., Schmidt F., Schumacher L.*, NStZ 2017, 7-8.
3. *Barrot W.,* ZJS 2010, 701-702.
4. *Barthe C., Gericke J., Diemer H.*, StPO, 9th ed. 2023, Section 152 StPO para. 4.
5. *Bechtold R., Bosch N., Brinker I., Bechtold R.,* EU-Kartellrecht, 4th ed. 2023, Regulation (EC) 1/2003, Art. 23 para. 91.
6. *Böse M., Satzger H.*, Europäisches Strafrecht (EnzEuR Bd. 9), 1st ed. 2013, § 2 para. 59.
7. *Böse M., Stuckenberg C.*, Europäisches Strafrecht (EnzEuR Bd. 11), 2nd ed. 2021, § 10 para. 17.
8. *Böttger M., Zoch S.,* Wirtschaftsstrafrecht, 3rd ed. 2023, ch. 17 Data Protection Criminal Law para. 282; *Gola,* CR 2018, 353 (355 f.).
9. *Brink S., Wybitul T.,* ZD 2024, 137 (142).
10. *Bülte J*, StV 2017, 460 (461).
11. *Calliess C., Ruffert M., Blanke H.*, EUV/AEUV, 6th ed. 2022, Art. 48 CFR para. 1-2, 4.
12. COM(2011) 573 final, 10; Council Doc. 16542/2/09 REV 2 No. 6-8.
13. *Dörr C., Grote H., Marauhn T.,* ECHR/GG, 3rd ed. 2022, ch. 14 para. 26.
14. *Drewes S., Walchner W.*, CR 2023, 163 (168).
15. *Dürig G., Herzog R., Herdegen M.,* GG (Vol. I), Art. 1 para. 36.
16. *Ehmann E., Selmayr M.,* DS-GVO, 2nd ed. 2018, Art. 58 DS-GVO para. 18, 27.
17. *Engelhart H.,* NZWiSt 2015, 201, 203.
18. *Engels H.*, Unternehmensvorsatz und Unternehmensfahrlässigkeit im Europäischen Kartellrecht, 2002, 71.
19. European Parliament resolution of 22 May 2012 on the EU approach to criminal law (2010/2310(INI)), C 264 E/9.
20. Explanations on the Charter of Fundamental Rights, OJ 2007 No. C 303/17, 30.
21. *Frister H.*, Schuldprinzip, Verbot der Verdachtsstrafe und Unschuldsvermutung als materielle Grundprinzipien des Strafrechts, 1988, 25, 89.
22. *Fromm E.*, ZIS 2007, 279, 287.
23. *Gassner K., Seith S.,* Ordnungswidrigkeitengesetz, 2nd ed. 2020, Introduction para. 6.
24. *Geco*, GA 2015, 503 (504).
25. *Gerhold S.*, 41st ed., Introduction to the OWiG para. 5.

26. *Globke*, in: *Brunhöber W., Höffler B., Kaspar F., Reinbacher R., Vormbaum M.,* (eds.) Strafrecht und Verfassung, 2012, 59, 66, 67.
27. *Gola P., Heckmann D.,* DS-GVO/BDSG, 3rd ed. 2022, Art. 83 DS-GVO para. 24.
28. *Grabenwarter C., Pabel K.*, ECHR, § 24 para. 19, 21, 22.
29. *Grabenwarter C., Pabel K.*, ECHR, 6th ed. 2016, § 24 para. 21.
30. *Grabitz E., Hilf M., Nettesheim M., Vogel P., Eisele J.,* Das Recht der Europäischen Union, 80th ed. 2023, Art. 83 TFEU, para. 46.
31. *Hassemer W.,* ZRP 2011, 192.
32. *Heckmann D.,* MMR 2023, 816 (818); in a different context on the validity of the principle of *ultra posse nemo obligatur* in data protection law *Hacker,* MMR 2018, 779, 784.
33. *Hochmayr G.*, ZIS 2016, 226, 230.
34. *Hörnle J.*, JZ 1999, 1080 (1088), is critical of the differentiation between criminal liability and criminal justification liability.
35. *Jarass H.*, CFR, 4th ed. 2021, Art. 48 para. 9, 12, 19.
36. *Karpenstein U., Mayer F.C.,* ECHR, 3rd ed. 2022, Art. 6 para. 25, 26.
37. *Keil G.*, Willensfreiheit, 2nd ed. 2013, 157.
38. *Klaas A., Momsen C., Wybitul T.*, Datenschutzsanktionenrecht, 1st ed. 2023, § 2 para. 22.
39. *Korte K.*, ZD-Aktuell 2024, 01500; https://www.lto.de/recht/hintergruende/h/eugh-c80721-deutsche-wohnen-dsgvo-bussgeld-erfolg-datenschutz-beauftragte-kartellrecht/ (last accessed on 1 March 2024).
40. *Kühling J., Buchner B., Bergt M.*, DS-GVO/BDSG, 4th ed. 2024, Section 41 BDSG para. 16.
41. KG Berlin BeckRS 2024, 2154; see on the question referred KG Berlin ZD 2022, 156.
42. *Meyer J., Hölscheidt S., Eser A., Kubiciel M.,* CFR, 5th ed. 2019, Art. 48 CFR para. 1, 6-7, 10, 13, 38.
43. *Meyer-Ladewig H., Nettesheim M., von Raumer S., Harrendorf H., König R., Voigt P.*, ECHR, 5th ed. 2023, Art. 6 ECHR para. 23-25.
44. *Mitsch W., Rogall K,* KK OWiG, 5th ed. 2018, OWiG § 30 para. 258, 270.
45. Opinion GA Carl Otto Lenz, 11 July 1992, Case C-143/91, EU:C:1990:381.
46. Opinion GA Juliane Kokott, 28 February 2013, Case C-681/11, EU:C:2013:126, para. 41.
47. *Paal B., Pauly D. A., Frenzel E.*, DS-GVO/BDSG, 3rd ed. 2021, Art. 83 DS-GVO para. 18-26.
48. *Parigger M., Helm T., Stevens-Bartol E., Müller R.,* Labour and Social Criminal Law, 1st ed. 2021, Section 42 BDSG para. 1.

49. *Pechstein M., Nowak R., Häde U., Schröder R.*, Frankfurter Kommentar EUV/AEUV/GRC, 2nd ed. 2023, Art. 49 para. 20.
50. *Rabe P.*, Das Verständigungsurteil des Bundesverfassungsgerichts und die Notwendigkeit von Reformen im Strafprozess, 2017, 147.
51. *Roxin C., Greco L.*, Strafrecht AT I, 2020, § 19 para. 9, 62.
52. *Satzger H.,* ZRP 2010, 137, 139.
53. *Schaut A.*, Europäische Strafrechtsprinzipien, 2012, 228.
54. S*chönke A., Schröder H., Eisele J.*, StGB, 30th ed. 2019, Vor. §§ 13 ff. para. 103.
55. *Schröter H., Jakob M., Klotz R., Mederer W., Kienapfel P.,* Europäisches Wettbewerbsrecht, 2nd ed. 2014, Art. 23 Kart-VO para. 39 f.
56. *Sieber U., Satzger H., von Heintschel-Heinegg F., Esser R.,* Europäisches Strafrecht, 2nd ed. 2014, § 55 para. 60, 63.
57. *Simitis S., Hornung G., Spiecker i., Petri T.,* Datenschutzrecht, 1st ed. 2019, GDPR Art. 4 No. 7 para. 23.
58. *Sydow G., Marsch N.* , DS-GVO/BDSG, 3rd ed. 2022, Art. 83 DS-GVO para. 2, 3 f.
59. *Tiedemann K.*, NJW 1993, 23, 28.
60. *Vogel P.*, JZ 1995, 331 (337).
61. *Wolff H. A., Brink S., von Ungern-Sternberg M. A.,* Data Protection Law, 46th edition 2021, Art. 83 GDPR para. 4.2.
62. *Zelger F.,* EuR 2021, 478 (481 et seq.).
63. BVerfGE 109, 133, 174 = NJW 2004, 739 (746).
64. BVerfGE 128, 326, 376 = NJW 2011, 1931 (1938).
65. BVerfGE 123, 267, 348 = NJW 2009, 2267 (2271).
66. BVerfGE 123, 267, 413 = NJW 2009, 2267 (2289).
67. BVerfGE 123, 267, 413 = NJW 2009, 2267 (2289).
68. BVerfGE 30, 1, 41 = NJW 1971, 275 (282).
69. BVerfGE 95, 96, 131 = NJW 1997, 929 (930).
70. BVerfGE 95, 96, 140 = NJW 1997, 929 (932).
71. ECJ judgement of 11 July 2002, Case C-210/00, ECR 2002 I-6453 para. 44 – *Käserei Champignon Hofmeister*.
72. ECJ judgement of 18.11.1987, Case 137/85, ECR 1987, 4587 para. 14 – *Maizena*.
73. ECJ judgement of. 16.11.1983, Case 188/82, ECR 1983, 3721 para. 18 – *Thyssen*.
74. ECJ NJW 2024, 343 para. 68.
75. ECJ, BeckRS 2012, 81043 para. 37 – Bonda.
76. ECJ, BeckRS 2018, 6055 para. 26 f. - Menci Luca.
77. ECJ, BeckRS 2018, 6055 para. 31.

78. ECJ, BeckRS 2022, 5011 para. 25 – bpost.
79. ECJ, BeckRS 2022, 5011 para. 26.
80. ECJ, BeckRS 2023, 24054 para. 49, 53.
81. ECJ, BeckRS 2023, 8994 para. 40, 42, 46.
82. ECJ, NJW 2024, 33, para. 45 - Volkswagen Italia SpA.
83. ECJ, NJW 2024, 343 para. 55, 60, 61, 62, 66, 67,70, 73, 74, 75, 78.
84. ECJ, NJW 2024, 343, 347 para. 68, 78 - Deutsche Wohnen.
85. ECtHR, BeckRS 1976, 107962 para. 81 f.
86. ECtHR, BeckRS 2010, 21072 para. 53 - Zolotoukhine v Russia.
87. ECtHR, BeckRS 2010, 21072.
88. ECtHR, BeckRS 2010, 2107253 - Zolotoukhine v Russia.
89. ECtHR, EuGRZ 1976, 221 - Engel et al. v Netherlands.

Otar Chakhunashvili*

Principles of Administrative Offense Proceedings in Assessing the Lawfulness of Personal Data Processing

The study of the lawfulness of personal data processing is one of the primary functions of the Personal Data Protection Service. This includes both the review of applications related to personal data processing and the examination (inspection) of its legality. This article explores the principles guiding the study of the lawfulness of personal data processing, which stem from the requirements set forth in the Law of Georgia "On Personal Data Protection" and the Code of Administrative Offenses of Georgia. These principles serve as the foundation upon which the Personal Data Protection Service evaluates each case.

Keywords: *Personal Data Protection Service, lawfulness of personal data processing, administrative offense case proceedings, principles of administrative offense case proceedings.*

1. Introduction

To properly conduct case proceedings when examining the lawfulness of personal data processing, it is crucial to adhere to principles explicitly established by applicable legislation or derived from the provisions of the Law of Georgia "On Personal Data Protection", the Code of Administrative Offenses of Georgia, and relevant subordinate normative acts.

According to Article 52 of the Law "on Personal Data Protection", if the Personal Data Protection Service detects an administrative offense, it is

* Doctor of Law, Assistant Professor at the Faculty of Law of Ivane Javakhishvili Tbilisi State University, First Deputy President of the Personal Data Protection Service of Georgia.

authorized to draw up a report of administrative offense and impose administrative liability on data controller and data processor, in accordance with the procedures established by this Law and the Code of Administrative Offenses of Georgia. Furthermore, Article 58, paragraph 3, of the same Law stipulates that the authority of the President of the Service and the procedure for conducting case proceedings are determined by this Law, the Code of Administrative Offenses of Georgia, other legislative acts, and normative acts issued by the President of the Service. Additionally, paragraph 4 of Article 58 establishes that in the event of a conflict between the Code of Administrative Offenses of Georgia and the provisions of this Law, the latter shall prevail.

The Law of Georgia "On Personal Data Protection", adopted last year, introduced several innovations, including newly established rules for imposing administrative liability for violations of the law. In contrast to the previous version, where administrative penalties were primarily imposed in accordance with the provisions of the Code of Administrative Offenses of Georgia, the updated Law of Georgia "On Personal Data Protection" now comprehensively outlines the rules that must be followed in case proceedings, taking into account the specifics of the field.

This paper examines the fundamental principles of case management in the study of the lawfulness of personal data processing, as reflected in the Law of Georgia on Personal Data Protection and the Code of Administrative Offenses of Georgia. Strict adherence to these principles is essential for reaching an appropriate decision in administrative offense cases.

2. Lawfulness

Article 39, paragraph 3, of the Law of Georgia "On Personal Data Protection" explicitly defines the principles governing the activities of the Personal Data Protection Service. The first and foremost of these principles is lawfulness, which requires that every action taken in the examination of the legality of personal data processing within administrative offense cases must strictly comply with the relevant legislative acts.

In performing its duties, the Personal Data Protection Service is guided by the Constitution of Georgia, international treaties, generally recognized principles and norms of international law, as well as this Law and other applicable legal acts**.**[1]

[1] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 39, Paragraph 2.

The Code of Administrative Offenses also upholds the principle of lawfulness in the imposition of sanctions for administrative offenses. According to Article 8, "No one may be sanctioned for administrative offences except on the basis of, and according to the procedure laid down by, the legislation. Proceedings for administrative offences shall be conducted with strict observance of the law. Authorised bodies and officials shall impose sanctions for administrative offences within their scope of authority, in strict compliance with the legislation."

Furthermore, Article 33 of the Code reinforces this principle by establishing the general rule for imposing administrative penalties. Specifically, it states that "A penalty for an administrative offence shall be imposed to the extent defined by the normative act that prescribes liability in strict compliance with this Code of Administrative Offences and other acts on administrative offences."

3. Protection of Human Rights and Freedoms

The principle of **protecting human rights and freedoms** is established in the very first article of the Law of Georgia "On the Protection of Personal Data." Specifically, the Law states: "The purpose of this Law is to ensure the protection of fundamental human rights and freedoms, including the right to the inviolability of private and family life, and to privacy and communication, in the processing of personal data."

Accordingly, at every stage of administrative offense proceedings, fundamental human rights and freedoms, as universally recognized by the Constitution of Georgia and international norms, must be strictly upheld.

4. Independence and Political Neutrality

The functions and duties of the Personal Data Protection Supervisory Authority are distinct among administrative bodies in Georgia, primarily due to its unique legal structure. A key defining factor is its independence and political neutrality, which are reinforced by both international and national legislation.

According to the General Data Protection Regulation (GDPR)[2] of the European Union, data protection supervisory authorities must operate with complete independence in the performance of their duties and the exercise of their powers. Similarly, under the Law of Georgia "On Personal Data Protection"**,** independence and political neutrality are fundamental principles of the authority's activities. Consequently, when examining the legality of personal data processing in administrative offense cases, employees of the Personal Data Protection Service must act independently and are strictly prohibited from using their official positions for political or party-related purposes.

This principle is further upheld in Article 55 of the Law, which guarantees the legal protection of employees of the Personal Data Protection Service. Specifically, the Law states: "No one has the right to interfere in the official activities of an employee of the Personal Data Protection Service, except in cases provided for by law". Also, "Obstructing an employee in the performance of their official duties, violating their honor and dignity, resisting them, making threats, committing acts of violence, or endangering their life, health, or property shall result in liability as established by Georgian law." Additionally, if there is credible information regarding threats to the life, health, or property of the President, First Deputy President, Deputy President, or any employee of the Personal Data Protection Service—or their family members—due to their official duties, state bodies are legally required to take measures to ensure their personal and property security".[3]

Moreover, obstructing the President of the Personal Data Protection Service or an authorized representative in the exercise of their legally defined rights constitutes an administrative offense under the Law of Georgia "On Personal Data Protection"[4], punishable by a fine ranging from 1,000 to 6,000 GEL**.** Additionally, any attempt to influence the President of the Service or an employee constitutes a criminal offense under the Criminal Code of Georgia and results in criminal liability.

[2] Personal Data Protection Service, European Union General Data Protection Regulation ("GDPR") - Georgian translation.
[3] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 55, Paragraph 3.
[4] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 88.

5. Objectivity and impartiality

Objectivity and impartiality are closely linked to independence and political neutrality, as discussed above. However, they constitute an independent principle and are explicitly recognized in the Law of Georgia on Personal Data Protection as a fundamental aspect of the Personal Data Protection Service's activities.

Notably, the current Code of Administrative Offenses does not explicitly define the principle of impartiality. However, the obligation to uphold it during proceedings can be inferred from Article 233 of the Code, which states: "Administrative proceedings shall be conducted based on the principle of equality of citizens before the law and the hearing authority (official), irrespective of origin, social and property status, racial or ethnic origin, sex, education, language, religious beliefs, type and nature of occupation, place of residence and other circumstances."

6. Proportionality

Every restrictive measure imposed by an administrative body must adhere to the principle of proportionality, which prohibits excessive or inappropriate restrictions on the subject of an administrative measure. This principle stems from the constitutional principle of a legal state, which permits the restriction of constitutional rights only to the extent necessary to protect public interests.[5]

When applying the principle of proportionality, the relationship between the means used by the administrative body and the intended goal must be carefully assessed. This evaluation follows a four-step process:[6] Determining the goal – Identifying the legitimate objective of the measure, Determining suitability – Assessing whether the chosen measure is appropriate for achieving the goal, Determining necessity – Evaluating whether a less restrictive alternative could achieve the same objective, Determining proportionality – Ensuring that the imposed measure is not excessively burdensome in relation to the desired outcome. These steps are extensively analyzed in Georgian legal scholarship.[7]

[5] *Detterbeck S.,* Allgemeines Verwaltungsrecht, 2004, 67.
[6] Ibid., 68-72.
[7] *Turava P., Tskepladze N.,* General Administrative Law Handbook, 2010, 27.

The proper application of proportionality is particularly important in administrative offense proceedings, especially when deciding on an appropriate administrative penalty or imposing a mandatory obligation on a data controller.

The significance of this principle is further reinforced by the European Data Protection Supervisor (EDPS), which has issued guidelines on proportionality in administrative measures. These guidelines emphasize that proportionality serves as a constraint on the exercise of authority, requiring a balanced approach between the means used and the objective pursued (or the result achieved).[8]

7. Equality Before the Law

According to the Constitution of Georgia,[9] *"all persons are equal before the law. Discrimination on the basis of race, skin color, sex, origin, ethnicity, language, religion, political or other opinions, social affiliation, property or rank, place of residence, or other grounds is prohibited."* This fundamental principle of equality is also enshrined in the General Administrative Code of Georgia. Specifically, Article 4 states that everyone is equal before the law and administrative bodies. It further establishes that: It is prohibited to restrict the legal rights, freedoms, or legitimate interests of any party engaged in administrative-legal relations, it is inadmissible to grant unlawful advantages or impose discriminatory measures against any party, and in cases where circumstances are identical, it is impermissible to render different decisions for different individuals**,** unless legally justified.

This prohibition of arbitrariness ensures that administrative bodies cannot apply unequal treatment to cases with substantially similar circumstances, nor can they treat substantially different cases as if they were the same. The incorporation of this constitutional principle into the General Administrative Code serves to safeguard the rights of individuals in administrative-legal relations. Any unjustified restriction or preferential treatment that lacks a reasonable legal basis constitutes a violation of this requirement.[10]

The principle of equality before the law is also reinforced in Article 233 of the Code of Administrative Offenses, which, as mentioned earlier, states that

[8] European Data Protection Supervisor, Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data, 2021, <https://edps.europa.eu> [10.02.2025].
[9] Constitution of Georgia, 1995, Article 11.
[10] *Turava P., Tskepladze N.,* General Administrative Law Handbook, 2010, 27.

administrative offense cases must be considered before the law and the responsible body (official) on the basis of equality for all citizens, regardless of their: Origin, Social or property status, race or nationality, Gender, education, language, religious beliefs, occupation, place of residence, or other circumstances.

This principle of equality is closely linked to the core principles outlined in the Law on Personal Data Protection, as discussed in this paper. Notably, the law recognizes professionalism as a key guiding principle of the Personal Data Protection Service. This means that employees of the Service must act based on professional knowledge, skills, and experience, ensuring that their decisions—particularly when assessing the legality of personal data processing—are made objectively, in the public interest, and strictly in accordance with legal requirements.

8. Protection of Secrecy and Confidentiality

The Law of Georgia on Personal Data Protection imposes an obligation on data processing organizations to ensure data security and requires them to determine the necessary organizational and technical measures to achieve this. Additionally, the law establishes the obligation of the controller, as well as the employee of the processor or has access to personal data, to strictly adhere to the limits of their granted authority and to protect the secrecy and confidentiality of data, including after the termination of their official duties.

Furthermore, data security is also ensured by employees of the Personal Data Protection Service, who are required to conduct their activities with full respect for secrecy and confidentiality. This obligation is explicitly stated in Article 51 of the Law on Personal Data Protection, which provides that an employee of the Personal Data Protection Service is required to protect the security of all types of confidential information and must not disclose any confidential information acquired in the course of official duties. This obligation remains in effect even after the termination of their authority. This requirement is further reinforced by Order No. 34 of the President of the Personal Data Protection Service, issued on March 1, 2024, "On Approval of the Procedure for Examining the Lawfulness of Personal Data Processing," which establishes confidentiality obligations as part of official procedural requirements.[11]

[11] Subparagraph "c" of paragraph three of Article 10 of the Order No. 34 of the President of the Personal Data Protection Service of March 1, 2024 “On Approval of the Procedure for Examining the Lawfulness of Personal Data Processing”.

9. Inquisitoriality

One of the defining features of administrative offense proceedings is the application of the inquisitorial principle by the body conducting the case. Although this principle is not explicitly defined in the Code of Administrative Offenses, it is inherent to administrative proceedings.

In general, the inquisitorial principle implies that the authorized body responsible for the case initiates administrative offense proceedings and actively investigates the matter on its own initiative. This body must assess both the circumstances that indicate an offense and those that exempt a person from liability, ensuring an objective and impartial evaluation of all relevant factors.[12]

The application of the inquisitorial principle by the Personal Data Protection Service in examining the lawfulness of data processing is a key characteristic of the sector. This is reflected in Chapter 7 of the Law of Georgia on Personal Data Protection, which defines the Service's powers in overseeing investigative actions related to data protection.

A primary function of the Personal Data Protection Service is to study the lawfulness of personal data processing. The Service is authorized to conduct inspections not only based on applications from interested parties but also on its own initiative[13]. This broad mandate allows the Service to actively engage in assessing data processing practices and ensures its inquisitorial authority. The Service initiates administrative offense proceedings either based on specific applications or publicly disseminated information. Additionally, at the beginning of each year, the President of the Service approves an annual inspection plan, which is developed by the Planned Inspection Department—a division established in 2023. In the same year, this department conducted 83 planned inspections to assess the legality of data processing.[14]

The purpose of the annual inspection plan is to enhance the effectiveness and consistency of the Service's activities, particularly in light of the diversity, dynamism, and complexity of modern data processing. The plan is formulated through a detailed study of data processing legislation and practices, the identification of priority and high-risk areas, and an analysis of risks associated with various data processing operations across different regions of Georgia.

[12] *Bohnert J.,* Ordnungswidrigkeitenrecht, 4th ed. 2010, 5.
[13] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 51, paragraph 1.
[14] Personal Data Protection Service. Personal Data Protection Service Activity Report for 2023. <https://pdps.ge/ka/content/988/angariSebi> [10.02.2025].

This approach ensures a targeted and efficient allocation of the Service's resources.[15]

The inquisitorial principle is also evident in the conduct of unplanned inspections, which are initiated by the Service to assess the legality of specific data processing activities. In 2024 alone, 182 unplanned inspections were conducted, further demonstrating the Service's commitment to proactive oversight and enforcement.[16]

10. Prohibition of Double Jeopardy ("ne bis in idem")

The risk of double jeopardy for an offender is a genuine concern in practice, despite its clear contradiction with universally recognized human rights. Punishing a person twice for the same illegal act is strictly prohibited, not only when penalties are imposed under different branches of law (e.g., the Criminal Code and the Code of Administrative Offenses) but also within the same legal framework. Once a penalty has been imposed, reapplying a sanction for the same offense is impermissible.

This principle, known as ne bis in idem, prohibits repeated punishment and is enshrined in Article 4, Part 1, of Additional Protocol No. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms. According to this provision, no individual may be tried or punished twice in criminal proceedings within the same State's jurisdiction for an offense for which they have already been finally acquitted or convicted in accordance with that State's legal and procedural standards. [17]

This approach is also firmly upheld in Georgian legislation. Specifically, Article 42, Paragraph 4 of the Constitution of Georgia states that no one may be convicted twice for the same offense. This constitutional provision reinforces the fundamental prohibition of double punishment, and its imperative nature means that no exceptions or limitations to this guarantee are permitted.

Furthermore, the Constitutional Court of Georgia has consistently reaffirmed the importance of the ne bis in idem principle. The Court has clarified that this principle serves a dual function: first, to protect individuals

[15] Personal Data Protection Service. Personal Data Protection Service Activity Report for 2023. <https://pdps.ge/ka/content/988/angariSebi> [10.02.2025].
[16] Personal Data Protection Service. Statistics on the activities of the Personal Data Protection Service for the 12 months of 2024, <https://pdps.ge/ka/content/988/angariSebi> [10.02.2025].
[17] European Convention on Human Rights, 1950.

from repeated criminal prosecution and punishment for the same act, and second, to ensure that state authorities are bound by final judicial decisions in criminal proceedings. [18]

The prohibition of double jeopardy is a fundamental manifestation of the rule of law. This principle ensures that state authorities, once they have rendered a final decision in a criminal justice process, cannot prosecute an individual again for the same act. This safeguard is directly linked to the principles of legal certainty and security. The predictability of legal consequences for actions that may restrict an individual's rights depends significantly on the extent to which final decisions in the justice system are upheld. If the law permits a person to be held liable multiple times for the same act and state authorities are not restricted in this regard, then the essential requirement that individuals must be able to anticipate the punishment for a specific act—and adjust their behavior accordingly—becomes meaningless.[19]

In the context of administrative offenses, the ne bis in idem principle is also recognized. Notably, under German administrative offense law, the prohibition of repeated prosecution applies in administrative proceedings as well.[20]

Similarly, Article 232 of the Administrative Offenses Code of Georgia explicitly upholds this principle. According to this provision, administrative offense proceedings cannot be initiated, and an existing case must be terminated if a competent authority (or official) has already imposed an administrative penalty on the person for the same act; an irrevocable decision has been issued by a civil court, following the transfer of materials from the body authorized to impose administrative penalties; an irrevocable resolution has been adopted to terminate the administrative offense case; a criminal case has been initiated on the same fact.

This principle is also explicitly enshrined in Order No. 34 of the President of the Personal Data Protection Service, issued on March 1, 2024, titled “On Approval of the Procedure for Reviewing the Lawfulness of Personal Data Processing.” Specifically, Article 18, Paragraph 1 outlines the circumstances that preclude the review of data processing legality, including:

[18] Decision of the Constitutional Court of Georgia No. 3/1/608,609 of September 29, 2015 in the case “Constitutional submission of the Supreme Court of Georgia on the constitutionality of Part 4 of Article 306 of the Criminal Procedure Code of Georgia and Constitutional submission of the Supreme Court of Georgia on the constitutionality of Subparagraph “g” of Article 297 of the Criminal Procedure Code of Georgia”, II-35 https://matsne.gov.ge/ka/document/view/3017013?publication=0 [10.02.2025].

[19] Decision No. 2/7/636 of the Constitutional Court of Georgia of December 29, 2016. <https://matsne.gov.ge/ka/document/view/3544820?publication=0> [10.02.2025].

[20] *Bohnert J.,* Ordnungswidrigkeitenrecht, 4th ed. 2010, 5.

- The existence of a court decision or ruling on the same fact of violation and involving the same parties, for which a review of the lawfulness of data processing should be initiated or is ongoing;
- The existence of a decision by the Service on the same fact and the same parties, for which a review should be initiated or is ongoing;
- The existence of a criminal case on the same fact, for which a review should be initiated or is ongoing.

11. Conclusion

This article examined the fundamental principles of administrative offense proceedings in the study of the legality of personal data processing, ensuring that these proceedings are conducted properly to protect the rights of data subjects.

The principle of lawfulness requires that every action taken in the proceedings strictly complies with legal standards. Without adherence to this principle, it is impossible to ensure that proceedings conform to both national legislation and international standards.

The protection of human rights and freedoms is not only essential in the study of personal data processing legality but also serves as a cornerstone of a lawful state.

The principle of independence and political neutrality acts as a key safeguard, ensuring that the study of personal data processing legality remains free from external influence, which is crucial for both justice and transparency.

Adhering to the principles of objectivity and impartiality prevents biased decision-making and serves as an essential guarantee of fair administrative proceedings.

The principle of proportionality ensures that all decisions are reasonable and appropriate, striking a balance between the rights of the data subject and public interests, while also preventing abuse of power.

The principle of equality before the law guarantees that all individuals enjoy the same rights and obligations, regardless of their social, legal, or other characteristics. This principle ensures that administrative decisions are based solely on legal grounds and not on unfair considerations.

The protection of secrecy and confidentiality is a fundamental aspect of the data processing process, extending even beyond the conclusion of a case. This obligation applies to both those responsible for processing personal data and employees of the Personal Data Protection Service.

The principle of inquisitoriality highlights the responsibility of administrative bodies to actively investigate all relevant facts, rather than relying solely on the information or documentation provided by the subject.

The principle of prohibition of double jeopardy (ne bis in idem) ensures that no individual can be held administratively liable twice for the same offense. This principle is vital for maintaining a fair legal environment, providing citizens with the assurance that they will not be subjected to excessive or unlawful sanctions. Its observance is crucial both for the protection of constitutional principles and the legitimacy of administrative proceedings.

In conclusion, strict adherence to each of the principles discussed in this article is essential for the effectiveness of administrative offense proceedings. Without these principles, it would be impossible to ensure the lawful protection of the rights of data subjects and to uphold justice and transparency in the administrative process.

Bibliography:

1. Constitution of Georgia, 24/08/1995.
2. Administrative Offenses Code of Georgia, 15/12/1984.
3. Criminal Code of Georgia, 13/08/1999.
4. Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.
5. Law of Georgia "On Personal Data Protection", 14/06/2023.
6. Order No. 34 of the President of the Personal Data Protection Service of March 1, 2024 "On Approval of the Procedure for Examining the Lawfulness of Personal Data Processing".
7. European Union General Data Protection Regulation ("GDPR").
8. *Bohnert J., Bülte J.,* Ordnungswidrigkeitenrecht. 5. Auflage. 2016.
9. *Detterbeck S.,* Allgemeines Verwaltungsrecht, 2004.
10. European Data Protection Supervisor, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, 2021.*
11. Personal Data Protection Service, Personal Data Protection Service Activity Report for 2023.
12. Personal Data Protection Service, Statistics on the activities of the Personal Data Protection Service for the 12 months of 2024.
13. *Turava P. Tskepladze N.,* General Administrative Law Handbook, 2010.
14. Decision of the Constitutional Court of Georgia of December 29, 2016 in case: №2/7/636.
15. Decision of the Constitutional Court of Georgia of September 29, 2015 in case №3/1/608,609.

Sergi Jorbenadze*

Scope of Personal Data Processing in Legal Practice

A lawyer processes a wide range of information in the course of professional activities, often involving a high likelihood of accessing personal data. In many cases, this includes special categories of personal data, requiring the lawyer to exercise heightened caution and adhere strictly to legal requirements. It is essential to distinguish between processing data for personal and professional purposes, ensuring data security, and safeguarding the client's interests.

Since legal practice does not grant unlimited mandate, unlawful processing of personal data by a lawyer can trigger a chain reaction. Specifically, a single action may not only violate personal data processing regulations but also breach professional standards.

This article focuses on the reconciliation and analysis of established practice, examining individual cases of violations of lawfulness or personal data processing standards within the context of legal practice.

Keywords: *Lawyer, personal data, data processing, professional standard.*

1. Introduction

In the course of their professional activities, lawyers often handle personal data, including that of both their clients and opposing parties. In this regard, lawyers (as well as their clients) are protected by Article 2, Paragraph 2, Subparagraph "d" of the Law of Georgia "On Personal Data Protection," which

* Doctor of Law, Associate Professor at the Faculty of Law, Ivane Javakhishvili Tbilisi State University, Lawyer.

exempts individuals from liability when processing personal data for the purposes of legal proceedings. However, this exemption should not be understood as granting lawyers absolute freedom in processing personal data. On the contrary, their actions, even when taken in the client's interest, may still violate the aforementioned law.

An interesting practice has developed in Georgia regarding the protection of personal data. In this context, there have been numerous cases in which the Personal Data Protection Service (hereinafter referred to as the Service) has reviewed individual applications and identified violations of the law. This work will primarily rely on the practice of the Service, which has encountered several noteworthy precedents. Two aspects should be noted in advance: a) for the purposes of this article, public information was requested from the Service. Accordingly, cases involving the appeal of the Service's decisions are not discussed herein[1]. Additionally, despite legislative changes,[2] the fundamental principles reflected in decisions made under the now-invalid law[3] remain relevant and are incorporated within the framework of the new law.[4]

2. The Scope of a Lawyer's Activities and Its Relation to Personal Data Protection

According to Article 1, Paragraph 2 of the Law of Georgia "On Lawyers," a lawyer must comply with the law and the norms of professional ethics. Additionally, Article 36 of the same law states: "If a lawyer commits an offense, he/she shall be held liable in accordance with the general procedure established by the legislation of Georgia." This provision does not limit a lawyer's liability solely to the Code of Professional Ethics. Rather, it also encompasses, for example, violations related to the disregard of personal data protection norms or other legal infractions.[5] The following example illustrates this point: when acting in the client's interest and fulfilling obligations under a

[1] Therefore, it is possible that a different approach may also be present in judicial practice.

[2] This refers to the Law of Georgia on Personal Data Protection, which was adopted on June 14, 2023, and published on July 3, 2023 (Document Number: 3144-XIმს-Xმპ, Registration Code: 010100000.05.001.020936), and is fully enacted at the time of the publication of this article.

[3] This refers to the Law of Georgia on Personal Data Protection, which was adopted on December 28, 2011, published on January 16, 2012, and whose date of repeal is March 1, 2024 (Document Number: 5669-რს, Registration Code: 010100000.05.001.016606).

[4] The new law is even more aligned with European standards, and it shares the substantive issues/principles that were in effect under the old law.

[5] Accordingly, a negative legal consequence may arise for the lawyer in proportion to each violation.

contract of assignment[6]—such as providing documentation or informing the client about a legal matter—a lawyer does not engage in misconduct. However, the manner in which the lawyer obtains and shares such information is crucial. A common example involves requests for public information. While the right to access public information is constitutionally guaranteed, it is essential to ensure that the content of such requests does not lead to the unlawful disclosure of personal data. In practice, there is a precedent where a lawyer submitted a request to a relevant body, seeking specific information. The request was accompanied by documentation that had been submitted by the opposing party in a court dispute, which contained personal data of individuals. As a result of the service's disclosure of this documentation, a violation was found.[7]

Of course, the above example does not mean that a lawyer is prohibited from requesting public information. On the contrary, a lawyer has the right to submit a request with the content they deem necessary, even if the requested information concerns an individual's personal data. Such an action does not, in itself, constitute a violation of the law.[8] In this regard, an interesting case arose in practice when a lawyer requested public information concerning a minor.[9] The public institution provided the lawyer with this information without obtaining the necessary consent from the relevant data subject.[10] As a result, the public institution failed to comply with the legislation and was found to be an offender by the Service.[11]

3. Separating Household Exemption from Professional Duties

What may be considered a client's personal goal may not necessarily align with a lawyer's personal goals. For example, if a lawyer violates confidentiality

[6] See the decision of the Personal Data Protection Service of Georgia, dated March 5, 2024, No. გ-1/046/2024.
[7] Decision of the Personal Data Protection Service of Georgia, dated June 30, 2024, No. გ-1/149/2023.
[8] A lawyer's desire may be to present such information as additional evidence in court. See the decision of the Personal Data Protection Service of Georgia, dated October 6, 2022, No. გ-1/130/2022 – whether the court will accept evidence obtained in this manner is a separate matter for dispute and consideration, and falls outside the competence of the Service.
[9] Special rules are provided by legislation regarding minors, and the issue is presented differently. For more on this issue, see *Khubulia N.,* Challenges in the Processing of Children's Personal Data, Journal of Personal Data Protection Law No. 1, 2024, 62-71.
[10] Neither from the legal representative nor, logically, from the minor.
[11] Decision of the Personal Data Protection Service of Georgia, dated February 20, 2023, No. გ-1/024/2023.

by disclosing details of a specific case that could identify individuals,[12] the consequences for the lawyer may differ from those for the client, even if the same action is taken.[13] Of course, it is essential to investigate whether any of the preconditions[14] or legitimate interests[15] outlined in Article 2, Paragraph 2 of the Law of Georgia on Personal Data Protection are genuinely applicable.

4. Scope of Actions Based on the Client's Interests

Protecting the client's interests is a lawyer's primary duty, which must be carried out in accordance with the law.[16] According to Article 6, Paragraph 1 of the Law of Georgia "On Lawyers," "*A lawyer has the right to use all means to protect the interests of a client that are not prohibited by legislation or professional ethics*." Therefore, the client must be protected in a manner that does not violate the law. This means that if a lawyer commits any misconduct, they will be held liable in accordance with the relevant legal provisions.[17]

a. The inadmissibility of violating the law, even if the circumstances of the dispute necessitate such action

Depending on the circumstances of the case, presenting additional evidence to the court may be necessary. This may require applying to a specific body, seeking clarification on an issue, or taking other relevant actions. However, acting solely in the client's interest does not justify a lawyer's actions if they violate the law.[18] For example, a case from recent practice involved a

[12] For consideration, see the decision of the Personal Data Protection Service of Georgia, dated August 5, 2022, No. გ-1/081/2022.
[13] Considering the combination of specific circumstances. See the decision of the State Inspector's Service of Georgia, dated April 21, 2020, No. გ-1/137/2020.
[14] See the decision of the State Inspector's Service of Georgia, dated June 15, 2021, No. გ-1/207/2021.
[15] See, for example, the decision of the State Inspector's Service of Georgia, dated April 28, 2020, No. გ-1/147/2020.
[16] See Article 5 of the Code of Professional Ethics for Lawyers.
[17] This could also be a crime outlined for by the Criminal Code.
[18] Since the combination of principles and grounds for data processing should be clearly defined. See, for example, the decision of the Personal Data Protection Service of Georgia, dated August 7, 2024, No. გ-1/191/2024.

lawyer who sent a letter to a governmental body, disclosing the marital status of a particular person. The Service determined that this action constituted a violation of the law.[19] Furthermore, during the proceedings, the Service requested the lawyer to disclose the source of the data included in the letter. Specifically, it inquired whether details such as marital status or family relationships were obtained from case materials, behavioral analysis, the client's statements, or other circumstances that justified such a conclusion. Additionally, the Service asked the lawyer to specify the means by which this information became available to him. Notably, the lawyer did not provide the requested information, which ultimately became a key factor in the Service's decision.[20]

b. Video and Audio Surveillance by a Lawyer

An interesting case arose in practice within the framework of legal proceedings: a lawyer's client had a telephone call with the opposing party in the lawyer's office. The conversation was conducted in "loudspeaker mode,"[21] meaning those around could hear it. Video and audio surveillance were conducted in the room where the conversation took place. Although the relevant information was recorded, the participant in the conversation was unaware of the recording, and the opposing party was not informed. Later, the opposing party discovered in the lawsuit filed in court that a reference was made to a conversation, the recording of which had not been consented to. As a result, the Service determined a violation of the law, including unlawful joint processing of personal data.[22]

[19] Decision of the Personal Data Protection Service of Georgia, dated July 7, 2023, No. ჵ-1/153/2023.
[20] According to Paragraph 3 of Article 51 of the Law of Georgia on Personal Data Protection, the Service has the authority to request information. Therefore, this does not contradict the second sentence of Paragraph 1 of Article 38 of the Law of Georgia on Lawyers: A lawyer shall independently carry out the practice of law. Any unlawful interference with a lawyer's activities, hindrance to a lawyer's work, improper influence on a lawyer by a state authority and/or another individual, intimidation, harassment, coercion, persecution, pressure, infliction of moral and/or material damage, violence or threats of violence, as well as any other act that may undermine the independence of the lawyer is prohibited.' This reasoning is provided in the decision.
[21] "Loudspeaker".
[22] Decision of the Personal Data Protection Service of Georgia, dated August 14, 2024, No. ჵ-1/198/2024.

c. Legality of Data Storage

Recording, storing, and disclosing a meeting (assembly) by a lawyer without obtaining the data subject's consent constitutes a violation of the law. In practice, there has been a case where a shareholders' meeting was recorded without the explicit consent of the attendees, and the recording was later disclosed. [23] While no legal violation was established for these two actions due to the statute of limitations, the law firm was held liable for storing the recording, as it was made without consent and retained unlawfully. From the service's standpoint, assessing the legality of evidence for procedural purposes falls outside its competence. However, if the law firm intended to present this recording as evidence in court, it should have been processed solely for legal proceedings. Furthermore, the recording should have been deleted immediately after serving its legal purpose, which did not occur in this case.

5. Connection with Professional Ethics Standards

In addition to violating personal data protection laws, a lawyer's actions may also breach the obligations outlined in the Code of Professional Ethics. For instance, publicly disclosing information about a colleague[24] or an opposing party,[25] as well as making insulting remarks, can constitute ethical violations.[26] In such cases, the lawyer's conduct will be evaluated separately within the framework of professional standards. Additionally, if the lawyer's actions involve identifying individuals and thereby violating the Law of Georgia on Personal Data Protection, the Service will independently assess the matter.[27]

[23] Decision of the Personal Data Protection Service of Georgia, dated October 6, 2022, No. გ-1/130/2022.

[24] Regarding unlawful actions publicly made against a colleague, see, for example, the decision of the Ethics Commission of the Georgian Bar Association, No. 078/23, dated July 31, 2024.

[25] Regarding unlawful actions toward the opposing party, see for example, the decision of the Ethics Commission of the Georgian Bar Association, No. 056/22, dated February 8, 2024; also, the decision of the Disciplinary Chamber of the Supreme Court of Georgia, No. სსდ-02-24, dated April 11, 2024.

[26] See, for example, the decision of the Ethics Commission of the Georgian Bar Association, No. 097/18, dated February 23, 2024; also, the decision of the Disciplinary Chamber of the Supreme Court of Georgia, No. სსდ-01-22, dated April 14, 2022.

[27] An illustrative case is when a lawyer filed a complaint with the Ethics Commission against a fellow lawyer for violating ethical standards and focused on such information (data) in the complaint, which resulted in a violation being established against him. See the decision of the Personal Data Protection Service, No. გ-1/153/2023, dated July 7, 2023.

The Ethics Commission of the Georgian Bar Association independently examines cases involving violations of the Code of Professional Ethics by lawyers. In this context, the Service reviewed the following case related to the activities of the Ethics Commission: The Chairperson of the Ethics Commission informed one of the collegiums in writing that a similar case was pending in another collegium and advised them to take this into account. A lawyer filed a complaint with the Service, arguing that the disclosure of such information constituted a legal violation. However, the Service determined that no legal breach had occurred, as the Chairperson of the Ethics Commission was authorized by law to take such action, which fell within their competence.[28]

6. Data Depersonalization by a Lawyer

Depersonalization of data is a crucial safeguard for protecting the data subject.[29] It involves processing data in such a way that the data subject cannot be identified, or identification would require disproportionate effort, cost, and/or time. This legislative provision (as outlined in Article 3, Subparagraph "c" of the Law of Georgia on Personal Data Protection) highlights the key principle: the data must not be recognizable by a third party. A common example of depersonalization is the use of initials; however, this alone does not necessarily ensure legal protection.[30] Two illustrative examples can be considered for discussion:

The first example involves information shared on social media by a law firm regarding a case that was resolved in favor of its client. The firm published details about the case, including the attorney's initials.[31] According to the service, this combination of information made it possible to identify the applicant. The service rejected the law firm's argument that identification was only feasible for a limited group of individuals (such as witnesses and family members of the parties involved). Instead, it concluded that the published details allowed the data subject to be identified without undue effort.[32]

[28] Decision No. ჹ-1/042/2024 of the Personal Data Protection Service of February 29, 2024.
[29] *Archuadze T.,* Depersonalization of Personal Data as a Guarantee of Data Subject Protection, Constitutional Law Review, No. 11 (2017), 101.
[30] For a detailed information on this issue, see there, 115.
[31] Specifically, information about the religious beliefs of the parties involved in the process, information about the residence of family members, etc.
[32] Decision No. ჹ-1/081/2022 of the Personal Data Protection Service of Georgia, dated August 5, 2022.

The second example involves a lawyer who filed a complaint with the Bar Ethics Commission against a colleague, also mentioning the colleague's spouse. While the lawyer's full name was provided, only the spouse's initials were used. Nevertheless, the service deemed this a violation. The reasoning was that, despite the use of initials, the complaint included additional details such as the spouse's profession, position at a company, work experience, completed exams, language proficiency, involvement in a dispute with the company, the subject of the dispute, and the office address. As a result, the combination of these details made it possible to identify the individual, undermining the effectiveness of depersonalization. Furthermore, the identification of the spouse had no legal relevance to the purpose of the complaint.[33]

7. Protection of Personal Data Security by a Lawyer

Lawyers (law firms) often store case files in their offices, where they may be accessible to various individuals, including colleagues and other employees. Frequently, the information handled by lawyers includes special categories of personal data, which require enhanced protection. [34] In this regard, service practice includes cases where lawyers and law firms have been instructed to implement organizational and technical measures to ensure data security. [35] Examples of such measures include storing physical files in a securely locked location, establishing a robust protection system for electronically stored data, and restricting public access.

8. Connection with Other Legal Institutions

Illegal processing of personal data may also infringe upon other rights of an individual. [36] A common example is the violation of non-property rights,

[33] Decision No. ჹ-1/153/2023 of the Personal Data Protection Service of Georgia, dated July 7, 2023.
[34] Moreover, its disclosure is not permitted. See, for example, the Decision No. ჹ-1/121/2021 of the State Inspector's Service of Georgia, dated April 26, 2021.
[35] Personal Data Protection Service's 2022 Activity Report, 109.
[36] In this case, it is necessary to distinguish between the violation of the right and the imposition of responsibility on the person. Therefore, for example, the professional standard of the lawyer will not be emphasized in this case.

which can manifest as defamation, insults, or similar offenses. [37] Even when a violation of non-property rights occurs alongside the unlawful processing of personal data, the service lacks the authority to examine such matters—particularly in determining the truthfulness or accuracy of the disseminated information. [38] In such cases, the affected party must pursue the issue individually, for instance, under the Law of Georgia "On Freedom of Speech and Expression." [39]

9. Conclusion

A lawyer (or law firm) must pay close attention to the issue of personal data processing. Legal activities are governed by the Law of Georgia "On Personal Data Protection," whether it involves self-advertising, disseminating information, or obtaining documentation. Additionally, a lawyer's actions may violate not only this law[40] but also the standards set forth in the Code of Professional Ethics,[41] among others. Georgian practice in this area has developed interestingly, with several decisions from the service outlining when a lawyer's actions were deemed to have violated the law.[42]

Therefore, a lawyer must carefully assess the scope of their authority to process personal data. A purely formal approach (such as depersonalization—where the data subject can still be identified—or relying on the client's interest) cannot serve as a valid defense against liability.

[37] See the decision of the Supreme Court of Georgia, dated October 22, 2020, No. ბს-921(კ-19).
[38] Personal Data Protection Service's Decision No. G-1/042/2024 of February 29, 2024.
[39] In relation to lawyers, considering their profession, the standard for freedom of expression cannot be the same as the standard set for representatives of other professions. See on this topic, Morice v. France [GC], [2015] ECHR, No. 29369/10, the Georgian Supreme Court's Ruling No. ას-1366-2019 of April 6, 2020, and the Georgian Supreme Court's Ruling No. ას-622-2022 of July 5, 2023.
[40] Accordingly, for the violation of the "Personal Data Protection Law" of Georgia, compensation for damages may be imposed, and this may be based on Articles 207 and 208 of the General Administrative Code of Georgia, as well as Articles 18 and 413 of the Civil Code of Georgia. For illustration, see the decision of the Supreme Court of Georgia dated July 11, 2023, №ბს-194(კ-23).
[41] See, for example, the decision of the Disciplinary Chamber of the Supreme Court of Georgia, dated November 5, 2024, №სსდ-09-24. Regarding lawyer advertising, see also *Khubuluri T.,* The Development of Legal Activity Advertising in the USA (19th-20th centuries), Ivane Surguladze 120, Anniversary Collection, Gegenava (Ed.), Tbilisi, 2024, 123-140
[42] See, for example, the decision of the State Inspector's Service, dated April 26, 2021, №გ-1/121/2021.

Bibliography:

1. Civil Code of Georgia, 786, 26/06/1997.
2. Criminal Code of Georgia, LHG, 41(48), 13/08/1999.
3. Law of Georgia “On Lawyers”, 976, 20/06/2001.
4. Law of Georgia “On Personal Data Protection”, 5669-რს, 28/12/2011.
5. Law of Georgia “On Freedom of Speech and Expression”, 220, 24/06/2004.
6. Law of Georgia “On Personal Data Protection”, 3144-XIმს-Xმპ, 14/06/2023.
7. *Archuadze T.,* Data Depersonalization as a Guarantee of Protection for Data Subjects, Review of Constitutional Law, №11, 2017, 101, 115.
8. *Khubulia N.,* Challenges in the Processing of Childrens Personal Data, Journal of Personal Data Protection Law, №1, 2024, 62-71.
9. *Khubuluri T.,* Development of Legal Advertising in the U.S. (19^{th}-20^{th} Centuries), Ivane Surguladze 120, Anniversary Collection, *Gegenava (ed.),* 2024, 123-140.
10. Personal Data Protection Service Annual Report for 2022, 109.
11. Decision of the Disciplinary Chamber of the Supreme Court of Georgia, April 14, 2022, №სსდ-01-22.
12. Decision of the Disciplinary Chamber of the Supreme Court of Georgia, April 11, 2024, №სსდ-02-24.
13. Decision of the Disciplinary Chamber of the Supreme Court of Georgia, November 5, 2024, №სსდ-09-24.
14. Decision of the Ethics Commission of the Georgian Bar Association, February 8, 2024, №056/22.
15. Decision of the Ethics Commission of the Georgian Bar Association, February 23, 2024, №097/18.
16. Decision of the Ethics Commission of the Georgian Bar Association, July 31, 2024, №078/23.
17. Decision of the Personal Data Protection Service, February 20, 2023, №გ-1/024/2023.
18. Decision of the Personal Data Protection Service, February 29, 2024, №გ-1/042/2024.
19. Decision of the Personal Data Protection Service, February 29, 2024, №გ-1/042/2024.
20. Decision of the Supreme Court of Georgia, April 6, 2020, №ას-1366-2019.
21. Decision of the State Inspector’s Service, April 21, 2020, №გ-1/137/2020.
22. Decision of the State Inspector’s Service, April 28, 2020, №გ-1/147/2020.

23. Decision of the Supreme Court of Georgia, October 22, 2020, №ბს-921(K-19).
24. Decision of the State Inspector's Service, April 26, 2021, №გ-1/121/2021.
25. Decision of the State Inspector's Service, June 15, 2021, №გ-1/207/2021.
26. Decision of the Personal Data Protection Service, August 5, 2022, №გ-1/081/2022.
27. Decision of the Personal Data Protection Service, October 6, 2022, №გ-1/130/2022.
28. Decision of the Supreme Court of Georgia, July 5, 2023, №ას-622-2022.
29. Decision of the Personal Data Protection Service, July 7, 2023, №გ-1/153/2023.
30. Decision of the Supreme Court of Georgia, July 11, 2023, №ბს-194(K-23).
31. Decision of the Personal Data Protection Service, March 5, 2024, №გ-1/046/2024.
32. Decision of the Personal Data Protection Service, June 30, 2024, №გ-1/149/2023.
33. Decision of the Personal Data Protection Service, August 7, 2024, №გ-1/191/2024.
34. Decision of the Personal Data Protection Service, August 14, 2024, №გ-1/198/2024.
35. *Morice v. France [GC]*, [2015] ECHR, №29369/10.

Beka Meladze*

Data Processing in Cloud Systems - Challenges and Opportunities

We live in an era where information drives every decision. Accurate and rapid data analysis fuels industries, shapes societies, and accelerates progress. At the heart of this transformation are cloud systems — revolutionizing how governments, businesses, and individuals operate. While this technology unlocks immense opportunities and streamlines daily processes, it also presents significant challenges, particularly in the legal and ethical processing of personal data.

Keywords: *Personal data, cloud systems, controller, processor, international data transfer, data security.*

1. Introduction

Cloud computing has emerged as one of the fastest-growing technologies of the past decade, revolutionizing data processing by surpassing the limitations of traditional physical infrastructure. By offering scalability, flexibility, and efficiency, cloud computing enables organizations to manage the ever-increasing volume of data in today's digital landscape. In 2024 alone, global spending on cloud computing services exceeded $600 billion[1], with projections nearing $1 trillion by 2027. This rapid growth is driven by widespread adoption across industries, as businesses recognize the cost-effectiveness and strategic advantages of cloud-based solutions[2].

* Master of Law (LL.M.) at Ivane Javakhishvili Tbilisi State University; Lawyer at the Private Sector Oversight Department, Personal Data Protection Service of Georgia.

[1] Public cloud services end-user spending worldwide from 2017 to 2024, <https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/> [21.02.2025].

[2] NexQloud will revolutionize the cloud technology market with a decentralized platform, 2024, <https://forbes.ge/nexqloud-set-to-disrupt-cloud-computing-with-decentralized-platform/> [21.02.2025].

While cloud computing offers flexibility and speed, it also introduces significant challenges in processing personal data through third-party servers. Key concerns include defining the roles and responsibilities of entities involved, ensuring data security, and addressing jurisdictional complexities related to data processing locations, which may impose various legal and regulatory obligations.

This paper explores the role of cloud systems in personal data processing, examining their capabilities while analyzing the challenges associated with confidentiality and security.

2. The Essence of Cloud Systems

Cloud systems enable individuals to utilize the infrastructure of service providers via the Internet, allowing them to store, manage, and process data from anywhere in the world.

In simple terms, cloud technology allows users to upload data, files, multimedia content, or applications to a provider's servers and access or modify them at any time, from any device. Today, numerous companies worldwide offer cloud-based solutions for various purposes. The leading providers in this field include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

According to the US National Institute of Standards and Technology ("NIST"), cloud systems have 5 characteristics[3]:

- On-demand self-service - Users can access and manage services at any time (e.g., opening and modifying their database) without requiring approval or assistance from the infrastructure provider;
- Broad Network Access - Data can be accessed, edited, deleted, or added from multiple devices simultaneously, ensuring seamless connectivity;
- Resource pooling - Service providers dynamically allocate infrastructure resources among multiple users based on demand, optimizing efficiency;
- Rapid elasticity - Users can scale resources up or down as needed, such as adjusting storage capacity on platforms like Google Drive;

[3] National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, Special Publication, 2012, 80-146.

- Measured Service – Costs are based on actual resource consumption, ensuring a flexible and usage-based pricing model.

It is important to note that cloud systems encompass a wide range of services, categorized into several key models:

- Software as a Service (SaaS) – Provides users with cloud-based applications, such as email and document storage services (e.g., Google Drive, Dropbox, Gmail, Outlook 365), eliminating the need for local installations.
- Platform as a Service (PaaS) – Offers a cloud-based environment for developers to build, test, and deploy applications without managing the underlying infrastructure (e.g., Google App Engine).
- Infrastructure as a Service (IaaS) – Primarily used by enterprises, this model allows organizations to utilize cloud providers' computing resources (e.g., servers, storage, and networking) instead of maintaining their own physical infrastructure.

It is important to note that, in accordance with Article 2, Paragraph 1 of the Law of Georgia "On Personal Data Protection"[4] the legislation applies to the processing of personal data through automated and semi-automated means within the territory of Georgia. Consequently, if an individual or entity processes personal data within Georgia—including cases where they merely access a cloud system—the provisions of the Law of Georgia "On Personal Data Protection" remain applicable. This holds true regardless of the physical location of the cloud system, the service provider, or the jurisdiction to which they belong[5] (For further details on cloud system locations and relevant jurisdictional considerations, see Chapter 5.1 of this article).

Despite the wide range of cloud system applications, Software as a Service (SaaS) stands out in the context of personal data processing. This model is of particular interest, as it is frequently utilized by data controllers for the storage, sharing, and processing of personal data.

[4] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023.
[5] EDPS, Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies, 2018.

3. Legal Status of Subjects

Data processing through cloud systems is a highly complex topic involving multiple parties. In many cases, due to the imbalance of resources and the dominant position of certain entities, it can be challenging to determine which party is responsible for data processing and which is authorized to process it. In this context, it is crucial to assess, on one hand, the role and responsibilities of the cloud service provider, and on the other hand, the responsibilities of the user of its services.

According to Article 3, subsection “o” of the Law of Georgia “On Personal Data Protection” data controller is the “natural person, a legal person, or a public institution, who individually or in collaboration with others determines the purposes and means of the processing of data, and who directly or through a processor processes data”, according to subsection "j" of the same article, data processor is “a natural person, a legal person, or a public institution, which processes data for or on behalf of the controller. A natural person who is in labour relations with the controller shall not be considered a processor”.

When utilizing cloud systems, the user determines the purposes and means of data processing, making them the data controller responsible for the processing. In contrast, the cloud service provider does not have a personal interest in processing user data and acts solely on behalf of the data controller. As such, the provider functions as the data processor**,** authorized to process data only in accordance with the instructions of the data controller[6].

It is important to note that, typically, in the data processing relationship, the data controller sets the "rules of the game," and the data processor follows them. However, when using cloud systems, the dominant role and resources of the service provider often mean that the data controller must accept the terms and conditions set by the provider. For instance, when a user opts to use Google Cloud Platform, they cannot dictate the terms for such a large-scale company. Nevertheless, the user still determines the purposes and means of data processing, which remains the key factor in determining their legal status as the data controller[7].

[6] The Data Protection Commission of Ireland: Guidance for Organisations Engaging Cloud Service Providers, 2019.

[7] Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].

4. Processing of Personal Data in Cloud Systems

Due to the efficiency of data processing, cloud systems are widely adopted by both businesses and government agencies. Additionally, cloud systems enable users to reduce costs and enhance service delivery.

Data processing through cloud systems can be broken down into several key stages. First and foremost, it is important to note that the data controller has the discretion to decide how, in what format, and to what extent data is uploaded to the cloud system.

The most common form of data processing in cloud systems is data storage ("Data at Rest"), where it is crucial to consider the security measures outlined in Article 27 of the Law of Georgia “On Personal Data Protection”. These measures must be implemented by both the cloud service provider and the data controller to ensure compliance and safeguard personal data.

In addition to storage, cloud systems are also utilized for various other types of data processing ("Data in Use"), such as downloading, sharing, analytics, and training artificial intelligence, among others. In these cases, the data controller must be aware that using a cloud system does not absolve them of the obligations set forth in the Law of Georgia “On Personal Data Protection”. This includes the duty to comply with both technical and organizational security measures, as well as, most importantly, to process data in accordance with the relevant legal basis and principles.

5. Challenges and Opportunities

It has been widely acknowledged that cloud systems enable companies and governments to process data efficiently and with flexibility. However, they also introduce several complex issues related to the legality of personal data processing. Among the most critical challenges are those concerning data security and the location of the systems.

5.1. The Location of Cloud Systems and the Aspect of International Data Transfer

A key distinguishing feature of cloud systems is that users can access the service provider's infrastructure and process data from anywhere in the world via the Internet. As such, when a data controller utilizes cloud systems, data may be stored or processed outside Georgia, as most cloud service providers,

including Google, Amazon, and Microsoft, operate databases and infrastructure in various countries[8]. In these cases, it is crucial to consider Article 37 of the Law of Georgia “On Personal Data Protection”, which allows the transfer of data to another country or international organization if certain conditions are met. Specifically, the transfer is permissible if the relevant jurisdiction or international organization provides adequate safeguards for data protection and the rights of the data subject, in accordance with the requirements outlined in the law.[9]

It is also important to note that Order No. 23 of the President of the Personal Data Protection Service, dated February 29, 2024, titled "On Approval of the List of Countries with Adequate Guarantees for the Protection of Personal Data,"[10] is currently in effect. This Order outlines a list of countries where data transfers are permitted without the need for additional justification.

In accordance with this legal framework, the data controller must first thoroughly investigate the country or countries where the data is being stored before proceeding with any data processing or transfer[11].

After obtaining the relevant information, if it is determined that data transfer occurs outside Georgia to a country not listed in the adequate guarantees list, the data controller is required to apply to the Personal Data Protection Service for authorization to transfer the data internationally[12]. Alternatively, the data controller must obtain written consent from the data subjects for the transfer.[13]

Regarding the international transfer of data through cloud systems, the decision of the European Data Protection Supervisor (EDPS) on March 8, 2024[14], is particularly noteworthy. In this decision, it was determined that the European Commission used the Microsoft 365 program, processing data through a cloud system, with servers located in the United States. As a result, international data transfers occurred without an appropriate legal basis.

[8] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 2012, 16.
[9] Law of Georgia “On Personal Data Protection”, 3144-XIMs-XMP, 14/06/2023, article 37.
[10] Order No. 23 of the President of the Personal Data Protection Service, dated February 29, 2024 “On Approval of the List of Countries with Adequate Guarantees for the Protection of Personal Data”
[11] Information Commissioner's Office (ICO) - Guidance on the use of cloud computing, version: 1.1, 18.
[12] It is important to note that international data transfer, upon obtaining permission, is one of the permissible grounds. Alternatively, depending on the specifics of data processing, other grounds may apply as outlined in Article 37, Paragraph 2 of the Law of Georgia on Personal Data Protection.
[13] It is mandatory that the written consent complies with the requirements set forth in Article 32 and Article 37, Paragraph 2, Subparagraph "d" of the Law of Georgia on Personal Data Protection.
[14] EDPS Investigation into Use of Microsoft 365 by the European Commission, Decision №2021-0518, 08/03/2024.

5.2. Data Security

According to Article 4 of the Law of Georgia "On Personal Data Protection", security constitutes one of the fundamental principles of data processing. Also, according to Article 27, „A controller and a processor are obliged to take organisational and technical measures that are adequate for the possible and associated risks of data processing (including data pseudonymisation, registration of the access to data, information security mechanisms (confidentiality, integrity, accessibility), etc.), which will ensure the protection of the data against loss or unlawful processing, including destruction, deletion, alteration, disclosure or use".

Based on the aforementioned provision, ensuring data security is the responsibility of both the processor — the cloud system provider — and the controller — the system user.

Given the specifics of the system, the primary responsibility for ensuring technical security lies with the service provider, i.e., the processor. Specifically, the provider must first ensure that the system is designed in a manner that prevents users from accessing each other's data. Additionally, the system must implement encryption technology utilizing a "Public Key" and "Private Key" mechanism, ensuring that the provider itself cannot access either stored data ("Data at Rest") or data in transit ("Data in Use")[15].

In practice, Georgian legislation primarily applies to cloud service users, i.e., controllers, as the operations of leading cloud service providers fall outside Georgia's jurisdiction.

Accordingly, it is crucial to determine the security-related obligations of controllers when utilizing cloud systems. First and foremost, controllers must thoroughly investigate and assess the security mechanisms of various cloud systems before selecting a reliable and secure provider[16].

Additionally, the cloud system user must implement organizational security standards and grant access to relevant data only to individuals who have the necessary authorization, legitimate grounds, and a justified need[17]. Furthermore, appropriate measures must be taken to prevent, detect, and mitigate unlawful data processing by employees, including ensuring that employees are adequately informed about data security matters.[18]

[15] CNIL, Recommendations for Companies planning to Use Cloud Computing Services, 2012, 10.

[16] Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 13-14, <https://ico.org.uk/> [10.03.2025].

[17] EU Data Protection Code of Conduct for Cloud Service Providers, 2020, 17-20.

[18] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 27 (6).

In accordance with Article 27(4) of the Law of Georgia "On Personal Data Protection", a controller is obliged to ensure that all operations performed in relation to electronic data (including information on incidents, data collection, data alteration, data access, data disclosure (transfer), data links and data deletion) are registered. In the vast majority of cases, cloud systems include a "logging" function; however, the controller is obligated to create multiple individual user accounts to ensure that, if necessary, it is possible to determine who specifically edited, deleted, added, or performed other actions on the data[19].

6. Conclusion

In conclusion, the increasing popularity of cloud systems is inevitable, as they represent one of the most advanced technologies for fast and flexible data processing, enabling companies, states, and individuals to reduce costs, enhance efficiency, and access data from anywhere in the world across various devices.

However, the capabilities of cloud systems are accompanied by significant challenges, particularly concerning the legal and ethical aspects of personal data processing.

To address these challenges, it is essential for both data controllers and authorized data processors to adhere to strict security measures. Specifically, the cloud service provider must implement robust data encryption technologies, while the user must ensure that access to data is granted only to authorized individuals and that all relevant organizational security standards are followed.

Furthermore, data controllers must determine the location of data storage and, if necessary, establish an appropriate legal basis for international data transfers.

Additionally, it is crucial to raise awareness of the intersection between cloud systems and data protection legislation, ensuring that data controllers fully understand both the advantages of cloud systems and the legal obligations they entail. Ultimately, personal data protection is not merely a technical legal requirement but a fundamental responsibility of any data processor.

[19] Information Commissioner's Office (ICO) - Guidance on the use of cloud computing, version: 1.1, 14 - 15.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023.
2. Order No. 23 of the President of the Personal Data Protection Service, dated February 29, 2024 “On Approval of the List of Countries with Adequate Guarantees for the Protection of Personal Data.
3. CNIL, Recommendations for Companies planning to Use Cloud Computing Services, 2012.
4. EDPS, Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies, 2018.
5. EDPS Investigation into Use of Microsoft 365 by the European Commission, Decision №2021-0518, 08/03/2024.
6. EU Data Protection Code of Conduct for Cloud Service Providers, 2020.
7. EDPS, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 2012.
8. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].
9. National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, Special Publication, 2012.
10. Public cloud services end-user spending worldwide from 2017 to 2024 <https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/> [21.02.2025].
11. The Data Protection Commission of Ireland: Guidance for Organisations Engaging Cloud Service Providers, 2019.

Giorgi Khorbaladze[*]

Video Monitoring of an Employee's Work Process/Space

The primary objective of the Law of Georgia "On Personal Data Protection" is to safeguard the rights to privacy, family life, personal space, and the inviolability of communication. Video monitoring constitutes one of the forms of personal data processing. To ensure the protection of an employee's rights as a data subject—particularly the right to personal autonomy—and to lawfully implement video monitoring of the workplace and work processes, it is essential to consider a range of legal aspects established under the Law on Personal Data Protection.

This paper examines the legislative framework governing the implementation of video monitoring in the workplace, alongside the relevant practices of the Personal Data Protection Service, supervisory authorities in European jurisdictions, and the European Court of Human Rights. Additionally, it addresses specific legal considerations pertaining to the video monitoring of employees' workspaces and work processes, as well as the key obligations of Controller to process such data.

Keywords: *Personal data, workspace/process, workplace, video monitoring, data security, impact.*

[*] Master of Law at Ivane Javakhishvili Tbilisi State University. Lawyer of the Office of the President of the Personal Data Protection Service of Georgia.

1. Introduction

The right to respect for private and family life is a fundamental human right enshrined in the Constitution of Georgia. The principle of personal autonomy is regarded as the cornerstone of the right to privacy[1], which is intrinsically linked to the concept of personal data as a critical component of this right. As long as individuals exist, personal data will exist. Consequently, in any democratic state, the protection of an individual's private life, as a supreme value, must be treated as a priority.

Despite the paramount importance of safeguarding private life, both national and international legal frameworks recognize that this right is not absolute. In certain circumstances, restrictions on this right are permissible. Given the inherently competing nature of human rights, it is essential to maintain a fair balance between them, necessitating a case-by-case assessment and analysis by the relevant authority or decision-maker. The right to the protection of personal data is frequently juxtaposed with the right to freedom of speech and expression. To ensure a fair equilibrium between these rights, the adjudicating body or individual must conduct a comprehensive examination of the specific circumstances and assess them in accordance with the principle of proportionality. A restriction imposed by the state on a fundamental right is justified only if it is prescribed by law, serves a legitimate aim, and is necessary in a democratic society.

One of the primary national legislative acts governing the protection of fundamental human rights and freedoms—particularly the rights to privacy, family life, personal space, and the inviolability of communication—is the Law of Georgia "On Personal Data Protection". Among other matters, this law regulates the processing of personal data through video monitoring in various private and public spaces. Given the broad scope of privacy protection, this study aims to examine a specific aspect of video monitoring—namely, the video monitoring of an employed individual's workspace and work process.

Accordingly, this study will analyze the legislative framework governing this issue, elucidate the concept of an employee's workspace and work process, and outline the standard of a reasonable expectation of privacy. Furthermore, the core section of the study will present relevant best practices derived from the Personal Data Protection Service, European Data Protection Supervisory Authorities, and the European Court of Human Rights.

[1] *Case of Pretty v. the United Kingdom*, [2002] ECHR App. No. 2346/02, §61.

2. Legislative Regulation of the Implementation of Video Monitoring

Video monitoring is the processing of visual image data using the technical means located/installed in a public or private space, including video control and/or video recording (except for covert investigative actions)[2].

Unlike the Law "On Personal Data Protection" that was in force on March 1st, 2024, the previous Law of December 28, 2011, did not explicitly include the concept of video monitoring, although it recognized video recording as a form of data processing. With the objective of aligning with European legislation, the new Law of Georgia "On Personal Data Protection" comprehensively regulates matters related to video monitoring, including the legal grounds for conducting video monitoring of an employee's workspace or work process.

Video monitoring constitutes a permissible form of personal data processing if it is conducted for specific purposes, such as the prevention and detection of crime, ensuring public security, protecting the safety of individuals and property, safeguarding minors (including protection from harmful influences), protecting confidential information, conducting examinations or testing, or fulfilling other tasks related to public and/or other legitimate interests. However, the implementation of video monitoring must be an adequate and proportionate means of achieving the intended purpose of data processing[3].

The purpose of implementing video monitoring in an employee's workplace may vary depending on the nature of the work process, the specific characteristics of the workspace, and other relevant factors[4]. In certain cases, based on the nature of the work being performed, the employer may even be obligated[5] to implement video monitoring[6]. Given the diverse and dynamic nature of labor relations, the current legal framework grants the personal data protection supervisory authority the discretion to assess, on a case-by-case basis, the legitimacy of an employer's interest in conducting video monitoring,

[2] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 3, subparagraph "g".
[3] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 10, Paragraph 1.
[4] For example, Article 20, Paragraph 17 of the Law of Georgia on General Education stipulates that video surveillance shall be implemented on the external and internal perimeters of schools for the purpose of ensuring the safety of individuals and protecting minors from harmful influences.
[5] See, for example, Order No. 1143 of the Minister of Internal Affairs of Georgia of August 29, 2007, "On the approval of video surveillance systems and the rules for their installation and operation at gambling and other profitable games (except for promotional draws) and on the external perimeters".
[6] *Takashvili S.,* Personal Data Processing Standards for Video Monitoring of an Employee's Workplace, Law Methods, №8, 2024, 129.

even when such an interest is not explicitly specified in the law but falls within the broader category of "other legitimate interests."

By contrast, the legal framework in force prior to March 1st, 2024, limited the permissible purposes for workplace video surveillance to personal and property security, the protection of confidential information, and the conduct of examinations or testing[7]. Thus, the current regulation under the Law "On Personal Data Protection" provides greater flexibility for assessment, enabling the resolution of complex legal issues in a lawful and equitable manner.

In the field of personal data protection, the Council of Europe Convention No. 108 of January 28, 1981, For the Protection of Individuals with regard to Automatic Processing of Personal Data, along with its modernized version, holds significant importance. The primary international legal instrument governing the processing of personal data is the European Union's General Data Protection Regulation (hereinafter referred to as the "GDPR"). Notably, while neither the aforementioned conventions nor the GDPR establish specific rules for processing personal data through video surveillance, they explicitly state that when processing data by such means, the Controller or Processor must comply with obligations to safeguard the dignity, legitimate interests, and fundamental rights of the data subject.

Accordingly, when assessing the lawfulness of processing an employee's personal data through video monitoring, data protection supervisory authorities (DPAs) rely on national legislation, European conventions, and the relevant provisions of the GDPR, which establish the principles and general rules governing personal data processing.

3. Employee's Workspace/Process

An employee, like an employer, is a party to an employment relationship. An employee is a natural person who, under an employment contract, performs specific work for an employer. Additionally, an employee may also hold the status of a public servant, as defined by the Law of Georgia On Public Service.[8]

[7] Law of Georgia "On Personal Data Protection", 5669-RS, 28/12/2011, Article 12, Paragraph 3.
[8] Organic Law of Georgia "Labor Code of Georgia", 4113-RS, 17/12/2010, Article 3, Paragraph 3. Also, according to Subparagraph "d" of Article 3 of the Law of Georgia "On Public Service", a public servant is a professional

The Law of Georgia On Labor Inspection provides definitions of an employee and their workplace/place of work. According to subparagraphs k and l of Article 3, a workplace is defined as a specific location where an employee directly performs labor activities, whereas a place of work encompasses all workplaces and the surrounding area where an employee or any other individual is present or moves for official purposes and which is directly or indirectly controlled by the employer[9]. A similar definition is found in Resolution No. 341 of the Government of Georgia, dated July 1, 2022, "On Approval of Technical Regulations on Minimum Requirements for Safety and Health Protection in the Workplace". This resolution also distinguishes between open and closed workspaces. However, due to the potential specificity of different workplaces and workspaces, various subordinate normative acts provide differing definitions of similar terms.[10]

With regard to the work process, it pertains directly to the employee's professional activities and may vary in terms of duration, the nature of the work performed, and other relevant factors. The work process may take place not only in enclosed spaces but also in open-air environments, as evidenced by a case examined by the Personal Data Protection Service concerning the legality of data processing for employees in a particular company[11].

According to the circumstances of the case, the company, through a processor, conducted video monitoring of employees working in outdoor spaces using security cameras, citing a high risk of harm to employee health as justification. During the investigation, it was established that these outdoor areas were designated for the execution of the employees' primary official duties and responsibilities. However, due to non-compliance with workplace video monitoring regulations—specifically, the company's failure to develop a written document governing the implementation of video monitoring—the company was found to be in violation of the law under Article 69 of the Law on Personal Data Protection. Accordingly, despite variations in work processes, the law provides equal protection for employees' personal data, ensuring compliance with established data protection standards.

civil servant/public official/civil servant, a person employed under an administrative contract, a person employed under an employment contract.

[9] See Recommendations on the Implementation of Video Monitoring and Audio Monitoring, 2024, 8.

[10] For example, Order No. 104/N of the Minister of Education and Science of Georgia of December 29, 2021, Article 3, Subsection "d".

[11] Decision No. G-1/340/2024 of the President of the Personal Data Protection Service of November 20, 2024.

4. The Standard of Reasonable Expectation of Privacy

The new Law “On the Personal Data Protection” expressly prohibits the implementation of video monitoring in any space where an individual has a reasonable expectation of privacy.[12]

The determination of a reasonable expectation of privacy is not based on the subjective perception of an individual but rather on the perspective of an objective observer or a third party[13]. In the workplace, such an expectation objectively exists in specific spaces, including areas designated for hygiene. Additionally, in cases where the nature of the work requires the presence of changing rooms, the Law on Personal Data Protection categorically prohibits video monitoring in such areas without exception. The implementation of video monitoring in these and similar spaces is deemed to be in violation of generally accepted moral standards. However, given the impossibility of exhaustively listing all such spaces under the Numerus Clausus principle, the legislator introduced the concept of a reasonable expectation of privacy as a guiding standard for assessing the permissibility of video surveillance in different workplace environments.

In addition to the aforementioned cases, an employee may also have a reasonable expectation of privacy in workplace spaces such as kitchens, where employees typically spend time during breaks. This expectation of privacy is equally reasonable in workplaces with day and night shifts, such as medical institutions or security companies, where rest areas are provided for employees[14].

"In certain environments, a person has a legitimate expectation of privacy and respect."[15] As a result, due to the heightened need for privacy in these spaces, the legislator explicitly prohibits video monitoring in such areas without exception. Consequently, Article 69 of the Law “On Personal Data Protection” imposes a stricter penalty in the form of a fine if the person responsible for data processing conducts video monitoring in an area where the data subject has a reasonable expectation of privacy.

[12] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 10, Paragraph 4.
[13] European Data Protection Board (EDPB), Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, Adopted on 29 January 2020, §36.
[14] For example, Order No. 06/n of the Minister of Education, Science, Culture and Sports of Georgia of January 29, 2019, “On the Approval of the Rules and Conditions for Maintaining Security and Public Order in a General Educational Institution,” establishes that video surveillance is prohibited in school restrooms, changing rooms, classrooms, and teacher's rooms.
[15] *Case of Von Hannover v. Germany,* [2004] ECHR App. No. 59320/00, §51.

5. The Importance of the Ultima Ratio Principle in Video Monitoring of an Employee's Workspace/Process

According to Article 10, paragraph 3 of the Law “On Personal Data Protection”, video monitoring of an employee's work process or workspace is only permitted in exceptional cases, where the objectives defined by law cannot be achieved through other means or would require disproportionate effort. The legal and legitimate grounds for implementing video monitoring are outlined in Article 10, paragraph 1 of the law, including purposes such as the protection of personal safety and property, public safety, and others.

However, in order for video monitoring of the work process or workspace to be deemed lawful, the legislator sets higher standards. In addition to having a legitimate purpose, the person responsible for data processing must demonstrate that the intended objective cannot be achieved by alternative means or that using such alternatives would entail disproportionate effort. Therefore, video monitoring of the workplace or work process, as an Ultima Ratio, is permissible only in exceptional circumstances, where no other logical, less intrusive alternative exists that would justify interfering with the right to privacy.

For a practical examination of this issue, it is useful to analyze the legality of video monitoring implemented by a private school as part of a planned inspection conducted by the Personal Data Protection Service[16]. According to the circumstances of the case, video monitoring was carried out in the school's computer science classroom. The school representative explained that the purpose of the video monitoring was to protect property, ensure security, and identify individuals causing damage. Additionally, the monitoring was carried out for testing purposes as part of periodic educational projects.

During the inspection, it was revealed that the school had an agreement on a "Security Rule" with the Ministry of Education, which, among other matters, explicitly stated that video monitoring in classrooms was inadmissible. As a result, aside from the violation of this specific rule, the Service's assessment determined that video monitoring in the computer science classroom was not an adequate or proportionate means of achieving the stated objectives. The protection of property, security prevention, and identification of individuals responsible for damage could have been accomplished through alternative measures, which were already outlined in

[16] Decision No. G-1/342/2024 of the President of the Personal Data Protection Service of November 22, 2024.

contracts with teachers. These contracts included provisions for protecting material assets and the designation of a responsible person/supervisor for the items. Regarding the testing purpose, despite the fact that such an objective is explicitly mentioned in the first paragraph of Article 10 of the Law "on Personal Data Protection", it was determined that the goal of monitoring the testing process could only be effectively achieved by video monitoring the process directly. The video monitoring carried out before and after the testing, however, exceeded the stated purpose. Therefore, in accordance with Article 69 of the Law (regarding violations of video monitoring implementation rules), the school was found to be in violation.

An educational institution is a space where both pupils/students and employees (e.g., teachers, lecturers) are engaged in the learning process. As such, the spaces within these institutions simultaneously serve as workplaces for employees. Therefore, the purpose for implementing video monitoring must justify any interference with personal privacy. The European Court of Human Rights, in the case Antović and Mirković v. Montenegro, clarified that the auditorium is the workplace of lecturers, where they not only teach students but also interact with them and contribute to the development of their social identity. Since the supervision of the learning process was not a purpose expressly permitted by national legislation, and no genuine need to protect the safety of individuals was identified, the Court ruled that the video monitoring of auditoriums violated Article 8 of the European Convention on Human Rights.[17]

The importance of the *Ultima Ratio* principle is clearly demonstrated in another decision by the Personal Data Protection Service[18], in which a college (the controller) implemented video monitoring through cameras located in several auditoriums (including a workshop, sewing room, and integrated laboratory). The controller justified the monitoring of these spaces as a measure to protect expensive equipment and inventory. However, the decision emphasized that the auditorium, by its nature, serves as a learning space for students and a work space for teachers, where interactions extend beyond academic topics to include personal and general matters.

While the protection of property is considered a legitimate goal, the decision highlighted that there were alternative means to achieve this goal. Specifically, the college conducted an annual inventory, and the contracts with teachers included provisions making them responsible for the material property of the college. The same objective could have been achieved by

[17] *Case of Antović and mirković v. Montenegro*, [2017] ECHR App. No. 70838/13, §44, §55-§60.
[18] Decision No. G-1/346/2024 of the President of the Personal Data Protection Service of November 26, 2024.

designating a responsible person for the items, storing valuable inventory in secure spaces, and keeping records of their use and return. Consequently, video monitoring was deemed neither a necessary nor an adequate means of achieving the college's objective. Since video monitoring was not the only feasible means to achieve the stated goal, there was no legal basis for the installation of a video monitoring system. As a result, the college was instructed to discontinue video monitoring in the classrooms.

This special regulation regarding the admissibility of video monitoring in an employee's workspace or process arises from the need to protect the right to privacy, as well as the potential "dilutive effect"[19] it may have on other fundamental rights (such as the freedom of assembly). Therefore, in addition to the existence of a legitimate interest, video monitoring must also be an adequate and proportionate means of achieving the goal of processing employee data.

6. Main Obligations of the Data Controller and Processor

6.1. Obligation to Inform

Once the employer establishes a legal basis for implementing video monitoring in the workplace, as stipulated by the Law on Personal Data Protection, they, as the data controller or processor, shall be subject to several obligations. In accordance with Article 10, Paragraph 8 of the Law on Personal Data Protection, the data controller processor is required to place a clearly visible warning sign indicating the ongoing video monitoring[20]. Furthermore, in the case specified under Paragraph 3 of the same Article, the employer must additionally provide the employee with written notification detailing the specific purpose(s) of the video monitoring. Compliance with these requirements shall be deemed sufficient to ensure that the data subject is informed of the processing of their personal data.

Accordingly, the law unequivocally establishes that the processing of an employee’s personal data (visual images) through video monitoring is

[19] Recommendations on the Implementation of Video Monitoring and Audio Monitoring, 2024, 8.

[20] A warning sign about the ongoing video monitoring must contain an appropriate inscription, an easily understandable image about the ongoing video monitoring, and the name and contact details of the controller.

prohibited in a manner that prevents the data subject from being aware of such processing. Recognizing the significance of safeguarding the principle of transparency, the legislation imposes an even higher standard of information disclosure in cases where video monitoring is conducted in the employee's workplace or during work processes. In addition to the requirement to place a visible warning sign, the employer, as the data controller or processor, is further obligated to provide employees with written notification specifying the exact purpose(s) of the video monitoring. Consequently, failure to conduct data processing in adherence to the principle of transparency may lead to a situation where the employer's legitimate interest (e.g., ensuring the security of company property) is transformed into an unwarranted and unlawful objective[21].

The decision of the European Court of Human Rights in López Ribalda and Others v. Spain[22] holds significant importance in the context of an employer's failure to fulfill the obligation to inform an employee. According to the factual circumstances of the case, the applicants were employed as cashiers and consultants in a supermarket in Barcelona. In March 2009, the supermarket administration became aware of financial losses and, in an effort to identify the cause, decided to install video surveillance cameras. Some of the installed cameras were concealed, with their field of view directed towards the cashiers. While the company informed employees about the installation of visible cameras and placed a warning sign, it failed to notify them of the hidden cameras.

Over the course of several months, the employment relationship with 14 employees, including the applicants, was terminated due to the theft of company property. The Chamber of the European Court of Human Rights determined that Article 8 of the European Convention on Human Rights had been violated, as the employees were not fully informed about the surveillance, and a fair balance was not maintained between the right to respect for private life and the employer's interests. The respondent state appealed the decision to the Grand Chamber.

In its ruling, the Grand Chamber acknowledged that the supermarket was an open space and that transactions at the cash register were not of a private nature. However, it also recognized that the surveillance took place in the employees' workplace, raising the issue of a reasonable expectation of privacy. The Court noted that such an expectation is significantly diminished in areas

[21] *Article 29 Data Protection Working Party*, Opinion 2/2017 on Data Processing at Work, Adopted on 8 June 2017, 9.
[22] *Case of López Ribalda and others v. Spain*, [2019] ECHR App. No. 1874/13; 8567/13.

where official duties are performed in public, particularly in direct interaction with customers. Nevertheless, given that the surveillance lasted only ten days and that access to the recordings was restricted to a limited number of individuals, the interference with the employees' private life was deemed to be of low severity. Furthermore, the Court emphasized that if the employees had been informed about the surveillance, the employer's objective—identifying the cause of the theft—would not have been achieved.

The European Court of Human Rights underscored the paramount importance of informing employees and ruled that conducting covert video surveillance based on mere suspicion of misconduct was not justified. However, the Court also recognized that where there is a reasonable suspicion of employee misconduct resulting in significant financial damage, the employer may be justified in implementing such measures despite the general obligation to inform, provided that the actions are necessary to prevent the disruption of the company's operations. Accordingly, the interference with the right to privacy was ultimately deemed justified in this specific case.

The European Court of Human Rights did not establish a violation of the right to private life in another case with circumstances similar to those outlined in the aforementioned decision. This case concerned the covert video surveillance of an employee (a cashier) by the employer. The Court recognized the employer's objective—to safeguard its property and detect instances of theft—as a legitimate and substantial interest. Furthermore, it determined that this objective could not have been effectively achieved through other equally efficient means.[23]

Furthermore, the guidance issued by the UK Data Protection Authority ("ICO") on the lawful monitoring of employees stipulates that, in exceptional circumstances—such as for the prevention or detection of criminal offenses—covert video surveillance in the workplace may be permissible. However, such monitoring must be conducted strictly by authorized personnel, with due consideration given to the limited duration and scope of surveillance[24]. Additionally, a data protection impact assessment must be carried out[25]. Notwithstanding the stated purpose, covert video surveillance remains strictly prohibited in areas where employees have a reasonable expectation of privacy[26], such as restrooms, changing rooms, and similar locations.

[23] *Case of Köpke v. Germany*, [2010] ECHR, App. No. 420/07.

[24] *EDPS*, Video-Surveillance Guidelines, Brussels, 17 March 2010, 31-32 <https://www.edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> [16.12.2024].

[25] Workplace Monitoring: What Are Your Employees' Rights? <https://gdprinformer.com/gdpr-articles/workplace-monitoring-rights> [15.12.2024].

[26] Workplace Monitoring: What Are Your Employees' Rights? <https://gdprinformer.com/gdpr-articles/workplace-monitoring-rights> [15.12.2024].

Pursuant to the Law “on Personal Data Protection”, video monitoring of an employee’s workspace or work process may be conducted for the purpose of detecting a crime. However, the law does not provide for the possibility of covert video surveillance by the data controller or processor. Instead, it unequivocally establishes the obligation to inform employees in writing as data subjects. Covert video monitoring in the workplace constitutes a serious intrusion into private life and carries the inherent risk of unlawfully obtaining other types of information related to employees’ private lives[27].

Accordingly, in light of the precedential interpretations provided by the European Court of Human Rights in the aforementioned decisions—where covert video surveillance in the workplace was deemed permissible only in exceptional circumstances—it is advisable that such measures be undertaken not by the data controller or processor, but rather by law enforcement authorities, particularly when conducted for the purpose of detecting criminal offenses

The significance of properly informing the data subject is further highlighted by the consistent practice established by the Personal Data Protection Service[28], which dictates that non-functional video cameras in the workplace are not permissible. Specifically, if a video camera is installed but not operational, the employer is obligated to either remove the camera or conduct video monitoring in accordance with the procedures established by law, which prioritize the protection and respect of private life. In such cases, the employee is not informed that their visual image is not being processed as personal data. As a result, the employee may mistakenly believe that their personal data is being processed, which could lead to an unreasonable alteration of their behavior due to perceived surveillance.

By fulfilling the obligation to inform, the principle of transparency in data processing is upheld, and personal data will be processed lawfully, provided that the employee has full awareness that their workspace or process is indeed subject to video monitoring.

[27] It may lead to liability under the Criminal Code (e.g., infringement of information reflecting private life or personal data (Criminal Code, No. 2287, Article 157).

[28] Decision No. G-1/342/2024 of the President of the Personal Data Protection Service of November 22, 2024, 18.

6.2. Obligation to Develop a Written Document

In addition to the obligation to inform the data subject, it is imperative that the data controller or processor, in accordance with the principles set forth in Article 4 of the Law on Personal Data Protection, formally document the purpose and scope of video monitoring, the duration of such monitoring, the storage period of the video recordings, as well as the procedures and conditions for accessing, storing, and destroying the recordings. Furthermore, the mechanisms for safeguarding the rights of the data subject must also be established.

Beyond ensuring transparency in the data processing process through video monitoring, the employer is further obligated to: collect or obtain personal data solely for specific, clearly defined, and legitimate purposes[29]; and process the data only for the duration and to the extent necessary to fulfill the legitimate purpose[30]. These principles form the foundation of the employer's duty to clearly outline in writing the critical aspects related to video monitoring. Although the regulatory provision does not explicitly require the provision of this written documentation to the data subject, Articles 24 and 25 of the Law “on Personal Data Protection” nevertheless impose the obligation to inform the data subject about such matters, regardless of whether the data is collected directly from the data subject.

In addition to the above, one of the guidelines issued by the United Kingdom Data Protection Supervisory Authority (“ICO”) emphasizes that, when monitoring employees for the purpose of protecting personal data, it is essential for the employer to assess the need for a data protection impact assessment. If there is a likelihood of processing special categories of data in this process, the employer is required to conduct an impact assessment[31].

The data controller is obligated to create a written document when carrying out an impact assessment in accordance with the procedure approved by Order No. 21 of the President of the Personal Data Protection Service, dated 28 February 2024. As per the same order, a high probability of creating a threat to the fundamental rights and freedoms of employees as a result of data

[29] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 4, Paragraph 1, Subparagraph "b".

[30] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 4, Paragraph 1, Subparagraphs: "c"; "e".

[31] *ICO*, Guideline on Monitoring of Workers by Employers, 2023, p. 20; 35 <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf> [20.12.2024].

processing using new technologies, data categories, volumes, purposes, and means of data processing may arise when two cumulative conditions are met. Specifically, if, for example, profiling leads to an assessment of the quality of work performed by employees, or if systematic and large-scale monitoring of employee behavior or condition (including physical/health condition) is conducted[32]. Therefore, the employer must assess the need for a data protection impact assessment in accordance with the procedure outlined in the aforementioned order, and, should the specified conditions be met, the employer will be obliged to develop an impact assessment document.

6.3. Obligations Regarding Data Security

Another key obligation of the data controller/processor is to ensure data security. As a fundamental principle, data security requires that the controller/processor implement appropriate technical and organizational measures to protect the data against unauthorized or unlawful processing, accidental loss, destruction, and/or damage[33]. This principle forms the basis for the requirement in Article 10(5) of the Personal Data Protection Law, which mandates that the video monitoring system and video recordings be safeguarded against unauthorized access and use. The controller is obligated to ensure that each instance of access to the video recordings is recorded (referred to as "logging"), including the time of access and the username, thus enabling the identification of the person accessing the data.

The importance of the obligation to establish security measures was highlighted by the French data protection supervisory authority in one of its decisions, where it was emphasized that the employee video surveillance system should be secured with a sufficiently strong password, and access should be restricted to a limited number of individuals[34]. The controller/processor is required to regularly check the functionality of the

[32] Order No. 21 of the President of the Personal Data Protection Service of February 28, 2024, Article 5, subparagraphs "a" and "b".
[33] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 4, Paragraph 1, Subparagraph "f".
[34] CNIL, Employee monitoring: CNIL Fined AMAZON FRANCE LOGISTIQUE €32 Million, <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million> [10.12.2024].

video surveillance system and take appropriate action in response to instances of unauthorized access to the system.[35]

The Latvian Personal Data Protection Supervisory Authority reviewed a case concerning the video surveillance of employees' workspaces using "CCTV" cameras installed at the workplace. According to the facts of the case, a company employee shared a video recording with the data subject through various communication platforms, despite the company's internal regulations explicitly prohibiting employees from accessing and sharing video recordings. The supervisory authority clarified that the company had implemented technical and organizational measures to ensure data security. Therefore, the company, as the data controller, could not be held liable for the actions of an employee who intentionally violated the data security protocols established by the company.[36]

Article 27 of the Law on Personal Data Protection specifically addresses data security matters. In particular, paragraphs 1 and 2 of this article stipulate that the data controller is obligated to implement appropriate technical and organizational measures to ensure that data is processed in compliance with this Law and to be able to demonstrate such compliance. Furthermore, both the data controller and the processor are required to adopt organizational and technical measures that are appropriate to the potential and inherent risks of data processing, thereby ensuring the protection of data against loss, unlawful processing, including destruction, deletion, alteration, disclosure, or unauthorized use.

The significance of data security protection is further reinforced by the consistent practice established by the Personal Data Protection Service, which holds that, to establish non-compliance with data security requirements, it is not necessary to have an unlawful disclosure of data. It is sufficient if "the data controller fails to consider the risks associated with data processing and creates a risk of unlawful data processing through their actions or inaction."[37].

Finally, in conjunction with other obligations established by law, data security protection is critical in that, without adequate measures, there are risks of unauthorized access, disclosure, public exposure, and dissemination of personal data. Even in the event of such risks, the lack of proper data security creates the grounds for the imposition of administrative liability.

[35] <https://pdps.ge/ka/content/978/5263/ra-unda-vicodeT-videomonitoringis-Sesaxeb> [11.12.2024].
[36] World Practice, Personal Data Protection Service, 2024, September, 4.
[37] Decision No. G-1/340/2024 of the President of the Personal Data Protection Service of November 20, 2024.

7. Conclusion

The data subject's official, professional activities are an inherent and integral part of their private life. "In the course of their professional life, most individuals have a unique opportunity to develop their relationship with the outside world.[38]" Therefore, the protection of personal data, as a crucial aspect of the right to privacy, must be guaranteed in the workplace of an employed person.

This paper examines the legislative regulation of the workplace/process of an employed individual, clarifies the standard of reasonable expectation of privacy, the principle of Ultima Ratio, and outlines the obligations of the employer as the data controller/ processor. In addition to theoretical considerations, the paper evaluates the practices and significant clarifications provided by the Personal Data Protection Authority, supervisory authorities of European countries, and the European Court of Human Rights.

The study revealed that the Law on Personal Data Protection establishes high standards for safeguarding the rights of an employee as a data subject and permits video monitoring of the work process/space only in exceptional circumstances. Furthermore, it was determined that in areas of the workplace where an individual has a reasonable expectation of privacy, video monitoring is prohibited, regardless of the legitimate purpose the employer may have.

The Law on Personal Data Protection specifically protects the personal data of employees, and in this context, which is permissible only under certain conditions, it imposes numerous obligations on the employer as the data controller/processor. Persistent failure to adhere to these obligations, particularly in terms of data security protection, where there is merely a risk of personal data security breaches, constitutes an administrative offense and provides grounds for imposing administrative liability.

[38] Case of Bărbulescu v. Romania, [2017] ECHR App. No. 61496/08, §61.

Bibliography:

1. Organic Law of Georgia "Labor Code of Georgia," No. 4113-RS, 17 December 2010.
2. Law of Georgia "On Personal Data Protection," No. 3144-XIMs-XMP, 14 June 2023.
3. Law of Georgia "On Public Service," No. 4346-Ic, 27 October 2015.
4. Law of Georgia "On Labor Inspection," No. 7178-Ic, 29 September 2020.
5. Law of Georgia "On General Education," No. SSM-1330, 8 April 2005.
6. Order No. 21 of the President of the Personal Data Protection Service of 28 February 2024.
7. Order No. 104/n of the Minister of Education and Science of Georgia of 29 December 2021.
8. Order No. 06/n of the Minister of Education, Science, Culture and Sports of Georgia of 29 January 2019.
9. Order No. 1143 of the Minister of Internal Affairs of Georgia of 29 August 2007, "On the Approval of Video Surveillance Systems and the Rules for Their Installation and Operation in Places of Gambling and Other Profitable Games (Except for Promotional Draws) and on the External Perimeter."
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 Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.
11. Resolution No. 341 of the Government of Georgia of 1 July 2022, "On the Approval of Technical Regulations on Minimum Requirements for Safety and Health Protection in the Workplace."
12. Article 29 Data Protection Working Party, Opinion 2/2017 on Data Processing at Work, 2017, 9.
13. CNIL, Employee Monitoring: Fined AMAZON FRANCE LOGISTIQUE €32 Million, <https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million> [10.12.2024].
14. EDPB, Guidelines 3/2019 on Processing of Personal Data Through Video Devices, Version 2.0, 2020, §36.
15. EDPS, Video-Surveillance Guidelines, Brussels, 17 March 2010, 31-32 <https://www.edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> [16.12.2024].
16. ICO, Guideline on the Monitoring of Workers by Employers, 20-35 <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-

resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf> [20.12.2024].
17. Recommendations on the Implementation of Video Monitoring and Audio Monitoring, Personal Data Protection Service, 2024, 8.
18. *Takashvili S.,* Personal Data Processing Standard for Video Monitoring of an Employee's Workplace, Law Methods, No. 8, 2024, 129.
19. World Practice, Personal Data Protection Service, October 2023, 7–8.
20. World Practice, Personal Data Protection Service, September 2024, 4.
21. Workplace Monitoring: What Are Your Employees' Rights? <https://gdprinformer.com/gdpr-articles/workplace-monitoring-rights> [15.12.2024].
22. Decision No. G-1/346/2024 of the President of the Personal Data Protection Service of 26 November 2024.
23. Decision No. G-1/342/2024 of the President of the Personal Data Protection Service of 22 November 2024.
24. Decision No. G-1/340/2024 of the President of the Personal Data Protection Service of 20 November 2024.
25. *López Ribalda and others v. Spain*, [2019] ECHR, №1874/13; №8567/13.
26. *Antović and Mirković v. Montenegro*, [2017] ECHR, №70838/13, §44, §55-§60.
27. *Bărbulescu v. Romania*, [2017] ECHR, №61496/08, §61.
28. *Köpke v. Germany*, [2010] ECHR, №420/07.
29. *Von Hannover v. Germany*, [2004] ECHR, №59320/00, §51.
30. *Pretty v. the United Kingdom*, [2002] ECHR, №2346/02, §61.

Mariami Giorgadze*

Legal Regulation of Artificial Intelligence Systems and Challenges related to Personal Data Protection

The objective of this article is to examine the current legal framework governing artificial intelligence, as well as the prevailing challenges concerning fundamental human rights, particularly the right to privacy and the protection of personal data in the context of AI operation and development. This study further explores the complexities and international best practices related to the processing of personal data by and through artificial intelligence.

***Keywords**: Artificial intelligence, fundamental human rights, personal data, legal regulation, data protection.*

1. Introduction

The advancement of technology has played a pivotal role throughout human history, profoundly transforming everyday life. A notable example is the series of industrial revolutions, which have driven significant social and economic changes since the late 18th century[1]. This evolution represents a continuous sequence of technological advancements, and today, in the era of the Fourth Industrial Revolution, artificial intelligence (AI), as one of its key manifestations, has the potential to bring about systemic transformations across various scientific fields and in daily human life[2].

The concept of artificial intelligence as a machine capable of human-like thinking emerged in the latter half of the 20th century. In 1950, the English

* Master of Law (LL.M.) at Ivane Javakhishvili Tbilisi State University, Faculty of Law; Specialist at the Office of the President, Personal Data Protection Service of Georgia.

[1] *Stearns P. N.,* The Industrial Revolution in World History, 4th ed., Westview Press, 2013, 9-14.

[2] *Schwab K.,* The Fourth Industrial Revolution, Encyclopedia Britannica, 2023, <https://www.britannica.com> [10.01.2025].

scientist Alan Turing introduced the idea of creating a machine that could "think" at a human level through a learning algorithm, formulating the "Turing Test"[3]—a criterion for assessing whether a machine can replicate human thought processes[4]. Since then, AI has undergone multiple stages of development, including periods of waning interest, before reaching its current state of advanced capabilities[5]. An intriguing hypothesis presented in scientific literature suggests that the origins of modern artificial intelligence stem from a convergence of various distinct disciplines: philosophical inquiries into the relationship between human cognition and information processing, economic models for decision-making optimization, neuroscientific research into brain function and structure, and the mathematical and engineering advancements that have enabled the development of AI models as they exist today.[6]

Today, artificial intelligence and AI-driven technologies have become deeply integrated into various aspects of society and numerous scientific fields—what was once considered a "technology of the future" is now an integral part of reality. AI is widely utilized across social media, finance, education, and the medical sector[7]. Its global popularization has been significantly accelerated by the emergence of generative AI models, particularly ChatGPT[8].

The advancement of artificial intelligence systems holds great potential for enhancing and simplifying everyday life, as well as contributing to scientific progress. However, it is crucial to recognize that AI is not flawless, and in the context of automated decision-making, the risks to fundamental human rights intensify. AI models are developed and continuously refined through the processing of vast amounts of data, with decision-making and predictions often relying on information that includes personal data. Consequently, as artificial intelligence becomes the cornerstone of the world's technological future, it is imperative to remain vigilant in safeguarding individual rights—

[3] *Russell S. J., Norvig P.,* Artificial Intelligence: a Modern Approach, 4th ed., Pearson, 2021, 35-36.

[4] An examiner who communicates in writing with a machine and a real person must identify who is on the other side of the communication - a person or a machine that thinks like him. Additionally - Geeks for Geeks, Turing Test in Artificial Intelligence, <https://www.geeksforgeeks.org/turing-test-artificial-intelligence/> [16.09.2024].

[5] *Kingsley O. A.,* Artificial Intelligence Research: a Review on Dominant Themes, Methods, Frameworks and Future Research Directions, Telematics and Informatics Reports, Volume 14, 2024.

[6] *Russell S. J., Norvig P.,* Artificial Intelligence: a Modern Approach, 4th ed., 2021, 35-36.

[7] *Gleeson B.,* How AI Is Reshaping The Future Of Work Across Industries, <https://www.forbes.com/sites/brentgleeson/2024/12/03/how-ai-is-reshaping-the-future-of-work-across-industries/> [03.12.2024]

[8] ChatGPT is a product of OpenAI, which has gained significant global attention for its artificial intelligence products since 2020-2022. It is a so-called "chatbot" capable of communicating and generating information in a manner similar to human interaction.

particularly the right to privacy and the protection of personal data—of those who are part of this evolving digital society.

The growing relevance of artificial intelligence, alongside digital technologies more broadly, presents significant challenges concerning fundamental human rights. In this context, the actions taken by supervisory authorities within their mandates play a particularly crucial role. Notably, one of the key priorities outlined in the 2025 Plan[9] for Scheduled Inspections of the Lawfulness of Personal Data Processing, established by the President of the Personal Data Protection Service, focuses specifically on modern technologies—encompassing both private and public institutions[10]. This initiative holds substantial importance in shaping national standards for personal data processing, advancing legal and practical frameworks, and safeguarding the right to privacy in the era of rapid technological development.

Furthermore, the European Data Protection Board (EDPB), at its 102nd plenary session on February 11, 2025, resolved to establish a Task Force on Artificial Intelligence[11], underscoring the increasing global attention on data processing by AI systems.

This paper examines the concept of artificial intelligence, the current state of legal regulations in this field, the existing and anticipated challenges posed by AI-driven technologies—particularly concerning personal data protection—and the critical considerations that must be addressed when processing data through artificial intelligence.

2. The Concept and Legal Regulation of Artificial Intelligence

2.1. The Concept of Artificial Intelligence: Systems and Models

The term “artificial intelligence” and its emergence as a distinct scientific field are linked to the 1956 Dartmouth Conference, where a group of researchers[12] sought to explore ways in which “machines could use language,

[9] Order No. B/1259 of the President of the Personal Data Protection Service of December 31, 2024 "On Approval of the Plan for Scheduled Inspections of the Lawfulness of Personal Data Processing for 2025".
[10] Ibid., Appendix №1 and №2.
[11] European Data Protection Board (EDPB), EDPB Adopts Statement on Age Assurance, Creates a Task Force on AI Enforcement and Gives Recommendations to WADA, <https://www.edpb.europa.eu/our-work-tools/plenary-meetings/102nd-plenary-meeting_en> [12.02.2025].
[12] John McCarthy (Assistant Professor of Mathematics, Dartmouth College), Marvin Minsky (Junior Fellow in Mathematics and Neuroscience, Harvard University), Nathaniel Rochester (Manager of Information Research, IBM Corporation), Claude Shannon (Mathematician, Bell Telephone Laboratories).Additionaly - History of Data Science, Dartmouth Summer Research Project: The Birth of Artificial Intelligence,

concepts, and abstractions to solve problems that were, at the time, considered uniquely human.[13]"

According to the modern definition, an artificial intelligence (AI) system is "a system based on machine technologies that, either explicitly or implicitly, analyzes how to generate outcomes—such as predictions, content, recommendations, or decisions—based on the information provided to it, which may influence the physical or virtual environment.[14]" Furthermore, AI systems exhibit varying degrees of autonomy[15] and adaptation during and after operation:

Autonomy – Refers to the extent to which an AI system can learn and operate independently, without human intervention, once granted autonomy and integrated into automated processes.

Adaptation – Denotes the system's ability to continue evolving beyond its initial development. This characteristic is particularly relevant to AI models based on machine learning, where the system refines its behavior through interaction with incoming data—such as a recognition system that adapts to an individual's voice over time.[16]

Machine learning is a model of artificial intelligence that replicates human learning through data and algorithms, enabling AI to make predictions and decisions based on new, similar data without requiring explicit programming for each specific task[17]. Various machine learning methods and algorithms are employed today, including linear regression, logistic regression, and decision trees, among others, each tailored to different types of data and problem-solving needs. Among these, one of the most widely used is the artificial neural network, which mimics the structure and functions of the human brain, allowing for the processing and analysis of complex data[18].

Deep learning, a subset of machine learning, utilizes multiple layers of neural networks (deep neural networks) and is capable of making decisions in

<https://www.historyofdatascience.com/dartmouth-summer-research-project-the-birth-of-artificial-intelligence/> [30.09.2021].

[13] McCarth J., Minsky M.L., Rochester N., Shannon C. E., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955, 2, <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>.

[14] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Article 3(1).

[15] Organisation for Economic Co-operation and Development (OECD), Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Artificial Intelligence Papers, №8, OECD Publishing, Paris, 2024.

[16] Ibid, 6.

[17] *Keskpaik S.,* Machine Unlearning, TechSonar Reports, 2024, 19, <https://www.edps.europa.eu/system/files/2024-11/24-11-15_techsonar_2025_en.pdf>.

[18] IBM, What is Artificial Intelligence (AI), <https://www.ibm.com/think/topics/artificial-intelligence?> [09.08.2024].

a manner akin to human cognition[19]. Leveraging specialized AI models—built upon foundational models such as Large Language Models (LLMs)—generative AI can perform various tasks, including the generation of text, images, and audio[20]. Prominent examples of such AI systems include ChatGPT, Gemini, Siri, and DALL·E 3, along with other widely recognized applications and platforms.

It is essential to emphasize that artificial intelligence models, while serving as fundamental components of AI systems, do not constitute AI systems in themselves. These models require additional elements—such as a user interface—to be integrated into a broader AI system[21]. The development of advanced and complex AI models is significantly influenced by the quantity, diversity, and quality of data used during the training process, which in turn affects the system's functionality and the challenges associated with it.

In addition to the numerous advantages of artificial intelligence highlighted thus far, AI also presents various risks. For instance, it may facilitate the spread of disinformation by generating synthetic content that humans perceive as real, or produce "hallucinations", where AI models convincingly convey false information. Bias and discrimination in AI-driven decisions and predictions, as well as data protection risks at different stages—including training, model operation, and human interaction—are also key concerns. Furthermore, AI presents challenges related to transparency and explainability, particularly in the case of so-called "black box" models, where decision-making processes remain opaque. The inability to appeal AI-generated outcomes and the risk of confidentiality breaches in cases of data protection incidents further highlight the need for a well-regulated and responsible approach to AI development and deployment.[22]

2.2. Legal Regulation of Artificial Intelligence

The challenges associated with the development and ethical use of artificial intelligence have led several modern nations to recognize the necessity of its legal regulation.

On August 1, 2024, the European Union's Artificial Intelligence Act entered into force. As the first legal regulatory framework for AI systems, it

[19] European Data Protection Supervisor (EDPS), Orientations for EUIs Using Generative AI, 2024, <https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf> [09.08.2024].
[20] European Data Protection Supervisor (EDPS), Orientations for EUIs Using Generative AI, 2024, <https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf> [09.08.2024].
[21] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Recital 97.
[22] *OECD*, AI, Data Governance and Privacy: Synergies and Areas of International Cooperation, OECD Artificial Intelligence Papers, №22, OECD Publishing, Paris, 2024.

aims to safeguard security, fundamental rights, and ethical principles throughout the development and deployment of artificial intelligence[23]. The regulation addresses key issues such as high-risk and general-purpose AI, establishes rules for their governance, defines prohibited uses of AI, and mandates the creation of AI-related supervisory bodies at various levels. The act is set to be implemented in stages, with its full enforcement scheduled for 2030.[24]

On September 5, 2024, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy[25], and the Rule of Law was opened for signature, with Georgia as a contracting party[26]. This convention represents the first legally binding international instrument designed to balance AI usage with human rights protections. It outlines the fundamental principles that AI systems must adhere to throughout their lifecycle. Furthermore, on November 28, 2024, the Council of Europe Committee on Artificial Intelligence (CAI) approved HUDERIA, a tool designed to assist both public and private institutions in assessing AI-related risks to ensure the protection of human rights, democracy, and the rule of law.[27]

In addition to the aforementioned legal acts, opinions, studies, instruments, and various guidance recommendations developed by international organizations play a crucial role in the legal regulation of artificial intelligence. Notably, the Organization for Economic Cooperation and Development (OECD) has made significant contributions in this area, with its definition of an artificial intelligence system closely aligned with the concept outlined in the EU Artificial Intelligence Act. The OECD conducts extensive research and analysis to examine the transformative impact of artificial intelligence on society and the economy[28].

The United Nations Educational, Scientific and Cultural Organization (UNESCO) is also actively engaged in AI-related matters, focusing on areas such as the ethics of artificial intelligence, the use of AI systems in education, and

[23] EDPS, Artificial Intelligence Act, <https://www.edps.europa.eu/artificial-intelligence/artificial-intelligence-act_en> [10.01.2025].
[24] <https://artificialintelligenceact.eu/implementation-timeline/> [01.06.2024].
[25] Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 225, 05.09.2024.
[26] Council of Europe (CoE), The Council of Europe Framework Convention on Artificial Intelligence, <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence> [10.01.2025].
[27] *Council of Europe (CoE) Committee on Artificial Intelligence (CAI),* Methodology for the Risk and Impact Assessment of AI Systems from the Point of View of Human Rights, Democracy and the Rule of Law ("The HUDERIA"), 28.11.2024, <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f> [09.08.2024].
[28] OECD, OECD Artificial Intelligence Papers, <https://doi.org/10.1787/dee339a8-en> [09.08.2024].

the intersection of artificial intelligence and gender equality, among other key issues.[29]

The United Nations (UN) continues to be actively involved in the development and regulation of artificial intelligence. An advisory body on artificial intelligence was established, and in March 2024, a resolution was adopted calling on states and other stakeholders to ethically develop, deploy, and operate AI systems, while ensuring the protection of human rights and freedoms[30].

In Georgia, the only existing legislation related to artificial intelligence is the 2020 Order of the President of the National Bank of Georgia, titled "On Approval of the Regulation on Risk Management of Data-Based Statistical, Artificial Intelligence, and Machine Learning Models". This order aims to establish a risk management framework for data-based statistical, AI, and machine learning models, promoting effective management of associated risks. It also outlines the process for building and using these models, particularly for entities under the supervision of the National Bank of Georgia[31].

Additionally, the Law on the State Budget of Georgia for 2025 includes plans related to artificial intelligence, including:

- Supporting the development of AI systems to benefit Georgian citizens and various sectors of the economy;
- Creating an international center of competence for AI, equipped with modern technologies and international expertise;
- Implementing AI systems to enhance the efficiency of the Ministry of Justice of Georgia's analytical and law-making activities, legal expertise of state contracts, and the conduct of proceedings in international courts and arbitrations, as well as providing simplified services to users of the Georgian Legislative Gazette;
- Studying and analyzing global AI trends, preparing conclusions and recommendations for adapting Georgian legislation to digital standards, and raising public awareness. Furthermore, the establishment of a Center for Legal Research on Artificial Intelligence is planned, based on the Training Center of the Ministry of Justice of Georgia.[32]

[29] *United Nations Educational, Scientific and Cultural Organization (UNESCO),* Artificial Intelligence, <https://www.unesco.org/en/artificial-intelligence> [09.08.2024].

[30] United Nations (UN), Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development, 11.03.2024, <https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf> [09.08.2024].

[31] Order No. 151/04 of the President of the National Bank of Georgia of August 17, 2020 "On Approval of the Regulation on Risk Management of Data-Based Statistical, Artificial Intelligence and Machine Learning Models".

[32] Law of Georgia "On the State Budget of Georgia for 2025", 45-Ims-XImp, 10.12.2024, Article 15, §3 and §6.

Based on these developments, it is clear that artificial intelligence is not only one of the most trending fields of modern technology at the international level, but at the national level, the state is highly committed to promoting its integration across various sectors. This signals that the challenges posed by AI are not only a current concern, but its active integration into multiple fields will likely amplify its impact on fundamental human rights and freedoms.

3. Challenges related to the Processing of Personal Data by Artificial Intelligence

3.1. Data Processing by/through Artificial Intelligence and the Role of Data Supervisory Authorities in Regulating Systems

As previously noted, artificial intelligence (AI) systems require large amounts of data for their creation, development, and use, often involving the processing of personal data[33]. Under both international (e.g., the GDPR, Convention 108)[34] and national legislation (Georgian Law on Personal Data Protection), data processing includes any operation performed on data, such as collection, retrieval, interconnection, or grouping.[35]

AI systems may process personal data at various stages, including design, marketing, operation, and development. If personal data processing is required—such as for machine learning—it falls under data protection regulations. Additionally, an AI system may itself contain personal data, and its distribution may constitute processing if such data is disclosed to third parties.

AI can also be used for automated decision-making and profiling. For example, in resume filtering, where personal data is processed automatically, potentially leading to legal or other significant consequences[36].

[33] Personal data is “any information relating to an identified or identifiable natural person.” See Law of Georgia “On Personal Data Protection”, 3144-XIMs-XMP, 14.06.2023, Article 3, subparagraph “a”.

[34] 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 Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.

[35] Ibid Article 3, subparagraph "f".

[36] *Agencia Española de Protección de Datos (AEPD),* Legal Report 0059/2023 of the Legal Office of the AEPD Ruling on the Difference Between AI Systems and Processing of Personal Data and the Assessment of the Level of Risk of Processings, 2023, <https://www.aepd.es/documento/informe-juridico-0059-2023-en.pdf> [09.08.2024].

The use of artificial intelligence (AI) systems can be particularly significant in the medical field, enabling the rapid and accurate diagnosis of various conditions. In such cases, personal data may be collected through various devices, sensors, clinical equipment, or medical examinations. AI systems may process patient data during training, testing, and ongoing evaluation to enhance their functionality.

Typically, this involves processing special categories of data, which are more sensitive in relation to human rights and freedoms. As a result, such data is subject to specific regulations, necessitating depersonalization or pseudonymization to prevent the identification of individual patients [37].

Given the above, the involvement of data protection supervisory authorities in regulating artificial intelligence (AI) systems has become increasingly relevant. Today, a significant portion of the research and activities conducted by supervisory authorities and international data protection organizations focus specifically on AI. For instance, the UK's data protection supervisory authority, the Information Commissioner's Office (ICO), has designated AI as a priority area due to its high potential risks to individuals and their rights[38]. Similarly, the Spanish data protection supervisory authority, the Agencia Española de Protección de Datos (AEPD), has issued various recommendations on the use of AI in different contexts, such as biometric data processing[39]. Additionally, in some cases, supervisory authorities have evaluated instances of AI-driven data processing, which will be analyzed in the following chapters.

The 2023 Global Privacy Assembly (GPA) Resolution on Generative AI Systems emphasizes that data protection and processing principles form the fundamental basis for AI system development and operation. These principles include the lawfulness of processing, purpose specification and limitation of further use, data minimization, accuracy, transparency, security, accountability, the protection of data subjects' rights, and the prioritization of data protection by default before considering alternative approaches [40].

---

[37] *Council Of Europe (CoE) Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO),* Report on the Application of Artificial Intelligence in Healthcare and Its Impact on the "Patient–Doctor" Relationship, 2024, 7-8.

[38] Information Commissioner's Office (ICO), Our Work on Artificial Intelligence, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/> [09.08.2024].

[39] Agencia Española de Proteccion de Datos (AEPD), Innovation and Technology, <https://www.aepd.es/en/areas/innovation-and-technology> [09.08.2024].

[40] *Global Privacy Assembly(GPA),* Resolution on Generative Artificial Intelligence Systems, 45th Closed Session, 2023, 5-9, <https://www.edps.europa.eu/system/files/2023-10/edps-gpa-resolution-on-generative-ai-systems_en.pdf> [09.08.2024].

3.2. Key Issues related to Data Processing by Artificial Intelligence Systems

Both during the development of artificial intelligence (AI) systems and their subsequent use, the processing of data by these systems must be carefully considered. This includes information about various groups of individuals used in the training process—whether obtained from public sources or provided by users during system interaction. Additionally, when individuals or organizations process third-party personal data using AI technologies—such as in the banking sector for risk assessment, in employment services for evaluating candidates, in the medical field for timely disease diagnosis, or in law enforcement for identifying criminal activity—it is essential to uphold data processing principles. Furthermore, organizations must assess the legal basis for processing data in this manner to ensure compliance with relevant regulations.

3.2.1. Processing of Personal Data for the Development of Artificial Intelligence Models

The EU Artificial Intelligence Act establishes obligations and additional safeguards to ensure privacy and the protection of personal data throughout the entire lifecycle of an AI system. It emphasizes that personal data processing must adhere to the principle of data minimization and prioritize data protection as the default approach when developing new products or services before considering alternative methods. Furthermore, the Act requires providers to ensure compliance with these principles by implementing measures such as depersonalizing data, encrypting it, and utilizing technologies that allow AI systems to be trained without copying raw data or transferring it between parties.[41]

The processing of personal data by artificial intelligence (AI) presents various challenges. For instance, the growing demand for generative AI chatbots has highlighted the need to establish appropriate age restrictions.

[41] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12.7.2024, Recital 69.

Minors may be less aware of the risks associated with providing their personal data to such systems and may lack the ability to effectively safeguard their rights. According to UNESCO recommendations, the minimum age for using these systems should be set at 13 years[42]. Additionally, states must assess whether self-reported age verification is sufficient and ensure that providers of generative AI systems are held accountable in this regard. Furthermore, the responsibilities of parents and legal guardians in monitoring interactions between individuals under 13 years of age and AI systems should be clearly defined.

In one case involving data processing through an AI chatbot—designed to enhance users' emotional well-being, track character development, and assist in managing anxiety and stress—the data protection supervisory authority determined that processing minors' data could not be based on contractual performance. Given the absence of an effective age verification mechanism, the authority restricted the AI system's data processing for all users until the entity responsible for processing rectified the identified deficiencies.[43]

Artificial intelligence (AI) systems may process an unlimited amount of personal data, including both user-provided information and data collected during training. Therefore, it is essential to ensure data security by implementing all appropriate safeguards. For example, in 2023, a technical flaw in ChatGPT temporarily allowed users to interact with other users of the AI, leading to the exposure of personal data such as names, email addresses, and credit information. In this case, the supervisory authority held the controller accountable for failing to notify the incident and for not adequately assessing the legal basis for data processing during the training process, which was inconsistent with the obligation of accountability. Additionally, the privacy policy was only available in English and was not easily accessible to users, despite the AI system also processing the personal data of unregistered users. The company failed to disclose this in its policy document, thereby violating the principle of transparency[44]. These concerns are particularly significant in the context of AI-driven data processing, as a lack of awareness regarding the processing of personal data can limit fundamental rights, such as the right to appeal and the right to request information.

[42] UNESCO, Towards a human-centered approach to the use of generative AI, 2023, 21, <https://doi.org/10.54675/EWZM9535> [09.08.2024].

[43] *Garante per la Protezione dei Dati Personali (Garante)*, [2023], no. 9852214, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9852214> [09.08.2024].

[44] *Garante per la Protezione dei Dati Personali (Garante)*, [2014], no. 10085455, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_10085455> [09.08.2024].

Data serves as the foundation for any artificial intelligence (AI) system, and its quality directly influences the outcomes produced by these systems. Incorrect or biased data representation can result in unfair or biased decisions and predictions. Historical data used in the training process may carry age-old social stigmas and reflect past discriminatory practices[45]. In addition to these historical biases, discriminatory approaches may arise from the improper representation of the characteristics of social groups or other relevant information during the training of AI systems. Overall, the processing of data from individuals by such AI systems may be degrading or otherwise negatively affect the rights of the data subject to whom the system is applied.

In the context of artificial intelligence (AI) models, issues concerning the "anonymity" of AI models (meaning that the AI does not process data related to an identified or identifiable person) and lawful data processing (based on legitimate interest) are of particular importance.

According to the European Data Protection Board (EDPB), the "anonymity" of an AI system should be assessed on a case-by-case basis. The EDPB asserts that AI systems whose training involved personal data cannot be considered anonymous under any circumstances. For an AI system to be regarded as depersonalized, it is necessary to obtain (or be able to obtain) the personal data of the individuals whose data was used during the development of the AI model. Additionally, the probability of retrieving these data through queries to the system—whether intentionally or unintentionally—must be minimal, considering the reasonable expectations of the controller or another responsible party.

The opinion further emphasizes that the assessment of the data protection supervisory authority should be based on the documentation provided to demonstrate the anonymity of the model.[46]

Regarding the processing of data based on legitimate interest for the development and operation of AI models, the European Data Protection Board (EDPB) emphasizes that there is no hierarchy between the grounds for processing data, and data controllers must identify the appropriate legal basis for their processing activities. Additionally, a three-step test must be applied when assessing legitimate interest. This includes: (1) identifying the existence of a legitimate interest, (2) determining the necessity of the processing to

[45] *The Europol Innovation Lab,* An Observatory Report on AI and Policing the Benefits and Challenges of Artificial Intelligence for Law Enforcement, 2024, 32,
<https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf> [09.08.2024].

[46] *The European Data Protection Board ("EDPB"),* Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024, §43, <https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf> [09.08.2024].

achieve that interest, and (3) assessing the balance of interests between the legitimate interest and the rights and freedoms of the data subjects. [47]

It is important to note that legitimate interest must be (1) lawful, (2) clearly and specifically formulated, and (3) real (rather than abstract). In the case of artificial intelligence models, an example of a legitimate interest might be improving methods for identifying threats to an information system. The necessity of processing must be assessed in terms of (1) how useful the data processing is for achieving the legitimate interest and (2) whether there is a less restrictive way to achieve the same goal. When designing or developing AI methods, it is crucial to assess the proportionality of the data used—ensuring data minimization. When assessing the balance of interests, the categories of personal data, the context of the processing, and the potential impact on the rights of the data subjects should all be considered. Additionally, the reasonable expectations of the subjects regarding the use of their data must be taken into account.[48]

The EDPB opinion also highlights the need to implement appropriate measures to mitigate any negative impacts on the rights of the data subject. These measures differ from the mandatory provisions outlined in the General Data Protection Regulation and should be tailored to the specific characteristics of the AI model, its purpose, and the circumstances of the particular case.[49]

3.2.2. Processing of Personal Data through Artificial Intelligence

Depending on the purpose of artificial intelligence (AI), its conclusions or predictions may necessitate the processing of personal data of specific individuals. In cases where the use of modern technologies, based on the processing of personal data, may result in decisions that affect the individual, leading to legal or other consequences, there may be potential negative impacts on the fundamental rights and freedoms of the data subject. Consequently, individuals or entities using such technologies, as data controllers, have certain obligations, particularly with regard to personal data protection. In this context, it is essential to address issues such as

[47] *EDPB,* Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(F) GDPR, Version 1.0 (for public consultation), 2024, §12, <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> [09.08.2024].
[48] *EDPB*, Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024.
[49] Ibid.

transparency, accountability, lawfulness and fairness of the processing, data security, and conducting data protection impact assessments, among others.

The use of AI across various fields serves different purposes. For example, in the business sector, AI may be used to customize offers and services by analyzing user behavior; in the education sector, to facilitate processes and create personalized learning plans; in healthcare, to detect disease symptoms in a timely manner, diagnose conditions, and analyze diagnostics[50]; and in employment, to predict the likelihood of success in applying for a specific position based on personal information such as professional experience, education, and test results

In such cases, it is essential to first assess the legal basis that an organization may have for processing data through artificial intelligence (AI). For example, certain information about a user may be necessary to place an order or provide a service to them. However, a different legal basis may be required for further processing of this information through AI to analyze the subject's preferences. In most cases, this could be consent or legitimate interest. Additionally, if the basis for processing data through these technologies is the consent of the data subject, the subject should voluntarily give consent only after being provided with clear and understandable information. As for legitimate interest, this should be assessed individually in each specific case, with the criteria discussed in the previous chapter being considered. For example, in a decision by the Hungarian Data Protection Supervisory Authority, concerning a bank’s use of AI to analyze emotional elements of customer conversations to assess satisfaction, the subjects were informed about audio monitoring. However, they were not informed about the further processing of these recordings. The bank considered legitimate interest—quality control—as the basis for the data processing. The supervisory authority ruled that the processing of audio recordings of customers and employees using AI was unlawful. This decision was based on the fact that the legitimate interest assessment did not account for the proportionality of the processing. Furthermore, the users were not informed about the analysis of their voice, meaning they could not exercise their right to "opt out". Additionally, the impact assessment did not include mitigating measures to reduce the impact and risks to the rights of the data subjects. Based on these

[50] World Economic Forum, 5 Ways AI is Transforming Healthcare, <https://www.weforum.org/stories/2025/01/ai-transforming-global-health/> [22.01.2025].

factors, the supervisory authority determined that the processing of personal data of users and employees through AI was inconsistent with the law. [51]

When processing data using artificial intelligence systems, it is also crucial to consider the principle of data minimization. According to the recommendation of the UK supervisory authority (ICO), employment agents should assess the information collected by artificial intelligence when using systems in the course of their activities. They must ensure that only the minimum necessary information is collected for the purposes of processing and that this data will not be used by AI providers for different purposes[52]. This approach should also be applied to other data processing processes involving artificial intelligence.

Transparency is one of the most important principles of data processing, and it requires that data subjects be provided with information about the processing of their personal data in a concise, easily understandable language, with the information being easily accessible[53]. Adhering to this principle can be particularly challenging when processing data through artificial intelligence, as many machine learning models are "black boxes" and do not explain their predictions in a way that is understandable to humans[54]. Consequently, interpreting and explaining decisions made by AI systems may be difficult even for those directly working with them, which creates specific challenges for the data controller in fulfilling their obligations.

The fair and dignified processing of data is also a fundamental principle that must be respected in all processing activities. As mentioned in the previous chapter, since the performance of artificial intelligence systems relies on the data used in their training process, there is a significant risk that these systems may not adequately reflect the characteristics of all societal groups or may be based on historical data that contains various stigmas. This can later lead the data controller to make biased, discriminatory decisions when using the system. Artificial intelligence systems are characterized by both historical, social, and algorithmic biases[55]. For instance, an artificial intelligence system used in the field of employment, whose training process was based on resumes

[51] *Nemzeti Adatvédelmi és Információszabadság Hatóság* (*NAIH),* [2024], NAIH-85-3/2022, <https://gdprhub.eu/index.php?title=NAIH_(Hungary)_-_NAIH-85-3/2022> [09.08.2024].
[52] *ICO,* AI tools in recruitment, 2024, <https://ico.org.uk/media/about-the-ico/documents/4031620/ai-in-recruitment-outcomes-report.pdf> [09.08.2024].
[53] *Article 29 Working Party,* Guidelines on transparency under Regulation 2016/679, 2018.
[54] *Cynthia Rudin,* Stop Explaining Black Box Machine Learning Models for High Stakes Decisions And Use Interpretable Models Instead, Nature Machine Intelligence, VOL 1, 2019, 206–215, <https://doi.org/10.1038/s42256-019-0048-x> [09.08.2024].
[55] *Dr. Kris SHRISHAK,* AI-Complex Algorithms and effective Data Protection Supervision Bias evaluation, *EDPB,* Support Pool of Experts Programme, 2024, 5-6, <https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf> [09.08.2024].

predominantly from male candidates, may, when deployed, filter out female candidates and preferentially select male candidates.[56]

In relation to the processing of data by means of artificial intelligence, it is also important to consider that the data subject has the right not to be subject to a decision made solely by automated means, which produces legal or other significant effects on them, except in cases where there is consent from the subject, it is necessary for the performance or conclusion of a contract, or it is provided for by law or subordinate acts[57]. Therefore, in these cases, decisions affecting the data subject should not be based solely on the predictions or conclusions of the system and must involve human supervision.

Due to the increased risk to the rights of the data subject and the high risk of their infringement, a data protection impact assessment may be necessary before processing data using artificial intelligence systems. This provides an additional safeguard for the protection of the subject's rights and helps the data controller demonstrate accountability and the lawfulness of processing[58]. An organization that decides to process data through artificial intelligence must ensure the security of these systems, including through technical or confidentiality documentation of the technology, and conduct periodic supervision within the scope of its competence.

4. Conclusion

Artificial intelligence is currently at the forefront of modern technologies and holds significant potential for the advancement of various fields. The application of these systems across sectors such as education, healthcare, law enforcement, business, and other areas vital for societal development can serve a range of purposes depending on the specific needs of each sector. AI can simplify tasks, analyze information, assess risks, make decisions, or predict/diagnose in a shorter timeframe. Given its expanding capabilities, there has been an increasing need for legal regulation of AI globally, leading to the development of frameworks such as the European Union Artificial Intelligence Act and the Council of Europe Framework Convention on Artificial Intelligence.

[56] *Byrne A., Lee D., Le Q.,* Bias in AI: Tackling the Issues through Regulations and Standards, 2024, <https://publicpolicy.ie/wp-content/uploads/2024/10/Bias_in_AI.pdf> [09.08.2024].
[57] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14.06.2023, Article 19 (1).
[58] *ICO,* How to Use AI and Personal Data Appropriately and Lawfully, 2022, <https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf> [09.08.2024].

Moreover, the research and recommendations from various international organizations play a critical role in ensuring the ethical and human rights-compliant use of these systems. This lays the groundwork for creating and enhancing legal frameworks for these technologies and contributes to their effective implementation.

The creation of artificial intelligence systems requires a large volume of data, including personal data, with particularly high data demands in complex models. The processing of information about individuals by artificial intelligence is relevant not only during its training and development stages but may also encompass its entire "life cycle." Personal data processing can be carried out by organizations directly involved in artificial intelligence systems, as well as by data controllers who process data of individuals using artificial intelligence within the scope of their activities across various sectors. In many instances, this form of automated processing has the potential to pose threats to the fundamental rights of individuals.

When processing data using artificial intelligence, both individuals working with these technologies and organizations utilizing them must consider issues such as the legal basis for data processing, as well as the principles of minimization, transparency, fairness, purpose limitation, and security. Additionally, data protection regulations should be adhered to, particularly in cases involving decision-making through automated data processing. A data protection impact assessment should be conducted, especially when artificial intelligence is applied in sectors such as healthcare or in activities involving the processing of special categories of data. Furthermore, data subjects must be adequately informed, as failure to do so may result in the negligent restriction of their rights as data subjects.

Data protection supervisory authorities can play a crucial role in preventing and effectively addressing the negative impacts of data processing by artificial intelligence systems. It is important to emphasize the need for recommendation-type documents and policy guidelines related to these technologies. Furthermore, to mitigate the impacts of artificial intelligence systems and ensure their effective use—while safeguarding rights—it is essential to engage in various awareness-raising activities to inform the public. Such efforts will significantly contribute to reducing the negative consequences associated with these technologies.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023.
2. Law of Georgia "On the State Budget of Georgia for 2025", 10/12/2024.
3. Order No. B/1259 of the President of the Personal Data Protection Service of December 31, 2024 "On Approval of the Plan for Scheduled Inspections of the Lawfulness of Personal Data Processing for 2025".
4. Order No. 151/04 of the President of the National Bank of Georgia of August 17, 2020 "On Approval of the Regulation on Risk Management of Data-Based Statistical, Artificial Intelligence and Machine Learning Models".Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12/07/2024.
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence (EU AI Act), OJ L, 2024/1689, 12/07/2024.
6. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 225, 05.09.2024.
7. 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, 04/05/2016.
8. Agencia Española de Proteccion de Datos (AEPD), Innovation and Technology, <https://www.aepd.es/en/areas/innovation-and-technology> [20.02.2025].
9. *Agencia Española de Protección de Datos (AEPD),* Legal Report 0059/2023 of the Legal Office of the AEPD Ruling on the Difference Between AI Systems and Processing of Personal Data and the Assessment of the Level of Risk of Processings, [2023], <https://www.aepd.es/documento/informe-juridico-0059-2023-en.pdf> [20.02.2025].
10. *Article 29 Working Party,* Guidelines on transparency under Regulation 2016/679, 2018.
11. *Byrne A., Lee D., Le Q.,* Bias in AI: Tackling the Issues through Regulations and Standards, 2024, <https://publicpolicy.ie/wp-content/uploads/2024/10/Bias_in_AI.pdf> [20.02.2025].

12. *Council Of Europe (CoE) Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO),* Report on the Application of Artificial Intelligence in Healthcare and Its Impact on the "Patient–Doctor" Relationship, September 2024.
13. *Council of Europe (CoE) Committee on Artificial Intelligence (CAI),* Methodology for the Risk and Impact Assessment of AI Systems from the Point of View of Human Rights, Democracy and the Rule of Law ("The HUDERIA"), 28/11/2024, <https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f> [20.02.2025].
14. *EDPS*, Artificial intelligence Act, <https://www.edps.europa.eu/artificial-intelligence/artificial-intelligence-act_en> [20.02.2025].
15. *EDPB,* Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(F) GDPR, 2024, <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> [20.02.2025].
16. *Gleeson B.,* How AI Is Reshaping the Future of Work Across Industries, <https://www.forbes.com/sites/brentgleeson/2024/12/03/how-ai-is-reshaping-the-future-of-work-across-industries/> [03.12.2024].
17. Geeks for Geeks, Turing Test in Artificial Intelligence, <https://www.geeksforgeeks.org/turing-test-artificial-intelligence/> [16.09.2024].
18. History of Data Science, Dartmouth Summer Research Project: The Birth of Artificial Intelligence, <https://www.historyofdatascience.com/dartmouth-summer-research-project-the-birth-of-artificial-intelligence/> [30.09.2021].
19. Information Commissioner's Office (ICO), Our Work on Artificial Intelligence, <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/> [20.02.2025].
20. *Information Commissioner's Office (ICO),* How to Use AI and Personal Data Appropriately and Lawfully, 2022, <https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf> [20.02.2025].
21. *Information Commissioner's Office (ICO),* AI Tools in Recruitment, 2024, <https://ico.org.uk/media/about-the-ico/documents/4031620/ai-in-recruitment-outcomes-report.pdf> [20.02.2025].
22. IBM, What is Artificial Intelligence (AI)?, <https://www.ibm.com/think/topics/artificial-intelligence> [09.08.2024].
23. *Keskpaik S.,* Machine Unlearning, TechSonar Reports, 2024, <https://www.edps.europa.eu/system/files/2024-11/24-11-15_techsonar_2025_en.pdf> [20.02.2025].

24. *Kingsley O. A.,* Artificial intelligence research: A review on dominant themes, methods, frameworks and future research directions, Telematics and Informatics Reports, Volume 14, 1.1, 2024, <https://doi.org/10.1016/j.teler.2024.100127> [20.02.2025].
25. *McCarth J., Minsky M. L., Rochester N., Shannon C. E.,* A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 31.08.1955, <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf> [20.02.2025].
26. OECD, Artificial Intelligence Papers, <https://doi.org/10.1787/dee339a8-en> [20.02.2025].
27. *Organisation for Economic Co-operation and Development* (*OECD),* Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Artificial Intelligence Papers, №8, OECD Publishing, Paris, 2024.
28. *OECD*, AI, Data Governance and Privacy: Synergies and Areas of International Cooperation, OECD Artificial Intelligence Papers, №22, OECD Publishing, Paris, 2024.
29. *Russell S. J., Norvig P.,* Artificial Intelligence: A Modern Approach, 4th Global Edition, Pearson Education Limited, 2021.
30. *Rudin C.,* Stop Explaining Black Box Machine Learning Models for High Stakes Decisions And Use Interpretable Models Instead, Nature Machine Intelligence, Vol. 1, 2019, 206-215.
31. *Shrishak K.,* AI-Complex Algorithms and effective Data Protection Supervision Bias evaluation, EDPB, Support Pool of Experts Programme, 2024, <https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf> [20.02.2025].
32. *Schwab K.,* The Fourth Industrial Revolution, Encyclopedia Britannica, 31.05. 2023, <https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734> [10.01.2025].
33. *Stearns P. N.,* The Industrial Revolution in World History, 4th ed., Westview Press, 2013.
34. The European Data Protection Board (EDPB), EDPB Adopts Statement on Age Assurance, Creates a Task Force on AI Enforcement and Gives Recommendations to WADA, <https://www.edpb.europa.eu/our-work-tools/plenary-meetings/102nd-plenary-meeting_en> [12.02.2025].
35. *The European Data Protection Supervisor (EDPS), Orientations for EUIs Using Generative AI, 2024,*

<https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf> [20.02.2025].

36. *The European Data Protection Board ("EDPB"),* Opinion 28/2024 on Certain Data Protection Aspects Related to The Processing of Personal Data in the Context of AI Models, 2024, §43.
37. *The Europol Innovation Lab,* An Observatory Report on AI and Policing the Benefits and Challenges of Artificial Intelligence for Law Enforcement, 2024, <https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf> [20.02.2025].
38. *The Global Privacy Assembly,* Resolution on Generative Artificial Intelligence Systems, 45th Closed Session, 2023, <https://www.edps.europa.eu/system/files/2023-10/edps-gpa-resolution-on-generative-ai-systems_en.pdf>
39. UNESCO, Artificial Intelligence, <https://www.unesco.org/en/artificial-intelligence> [20.02.2025].
40. *UNESCO,* Towards a Human-Centred Approach to the Use of Generative AI, 2023, 21, <https://doi.org/10.54675/EWZM9535> [20.02.2025].
41. *United Nations (UN),* Seizing The Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development, 11.03.2024, <https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf> [20.02.2025].
42. World Economic Forum, 5 Ways AI is Transforming Healthcare, <https://www.weforum.org/stories/2025/01/ai-transforming-global-health/> [22.01.2025].
43. *Garante per la Protezione dei Dati Personali (Garante),* [2023], no. 9852214, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9852214> [20.02.2025].
44. *Garante per la Protezione dei Dati Personali (Garante),* [2014], no. 10085455, <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_10085455> [20.02.2025].
45. *Nemzeti Adatvédelmi és Információszabadság Hatóság* (*NAIH),* [2024], NAIH-85-3/2022, <https://gdprhub.eu/index.php?title=NAIH_(Hungary)_-_NAIH-85-3/2022> [20.02.2025].
46. <https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-foundation-models-are-developed> [20.02.2025].
47. <https://artificialintelligenceact.eu/implementation-timeline/> [20.02.2025].

Marika Abazadze*

Personal Data Protection in Scientific and Academic Research

With the enactment of the new Law of Georgia on Personal Data Protection, the need to balance a high standard of data security with the legitimate interest in processing data for academic research has become increasingly relevant. This article examines the legal aspects of personal data protection that researchers must consider when conducting scientific and academic studies. It explores key issues that arise in daily research activities and highlights relevant best practices.

Keywords: *Scientific and academic research, secondary data processing, validity of data subject consent, personal data security, data subject rights.*

1. Introduction

Scientific and academic research often involves collecting and storing information in both digital and physical formats. A key challenge in this process is ensuring that the use and sharing of personal data comply with data protection legislation.

The protection of personal data is a fundamental right of the data subject. Therefore, safeguarding personal data should be a priority from the very outset of academic research, including during the planning phase and when defining research objectives.[1] Notably, the concept of "confidentiality" can be

* Master of Law in Data Protection and Privacy - Dublin City University (DCU); Master of International Law - Georgian Institute of Public Affairs (GIPA); Researcher-Analyst in the Department of International Relations, Analytics and Strategic Development of the Personal Data Protection Service.

[1] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 5.

interpreted differently depending on cultural and contextual factors[2], making it essential to tailor data processing approaches to the specific research setting.

The research methodology should also be evaluated from a personal data protection perspective. For instance, in cases involving covert observation of data subjects, it is crucial to assess how the terms "public" and "private" apply within the research context. Such observation is permissible only if the researcher can clearly justify its necessity and demonstrate that achieving the research objectives through alternative methods would be extremely difficult or impossible. Additionally, the researcher must ensure that covert observation does not infringe upon the rights and freedoms of data subjects.

Compliance with personal data protection laws extends beyond defining research objectives and methodologies. It encompasses all stages of research implementation, including data collection, access, respondent communication, and data storage or erasure. Some institutions and organizations outline detailed data protection strategies that govern the entire data processing cycle, ensuring proper storage, accuracy, and security.[3]

Academic research may also involve international data transfers. While the General Data Protection Regulation (GDPR) seeks to standardize data protection rules across Europe, national regulations can introduce variations, particularly in the context of statistical or academic research. EU Member States have discretion in defining and regulating scientific research, leading to potential legal discrepancies that may complicate international data transfers and research collaborations.[4]

In Georgia, the Law on the Protection of Personal Data allows personal data processing for research purposes, provided that appropriate technical and organizational security measures are in place to safeguard the rights of data subjects. Furthermore, data controllers must comply with all relevant legislative requirements.[5]

[2] Law of Georgia "On Personal Data Protection", Article 27 (2).

[3] *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021.

[4] *Ducato R.,* Data Protection, Scientific Research, and the Role of Information, Computer Law & Security Review, Vol. 37, 2020, 14.

[5] Law of Georgia "On Personal Data Protection", Article 4(6).

2. Principles and Activities of Personal Data Processing

According to the Law of Georgia "On Personal Data Protection", any action involving personal data constitutes data processing. In the context of research projects, data processing includes activities such as compiling respondent email lists, creating and managing databases, and sharing data with third parties. The law defines "processing of personal data" as any action or set of actions performed on personal data, regardless of the form or means used. This includes both automated and non-automated processing methods, such as collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, transmission, dissemination, rectification, combination, blocking, erasure, or destruction.[6]

The consent of the data subject introduces different obligations depending on the field of application. In scientific or clinical research, for instance, at the data collection stage, the data controller may not always be able to define a single, specific purpose for data processing.[7] The relevant regulations acknowledge this challenge and allow data subjects to consent to data processing for broader research purposes, considering the scope and context of the processing.[8]

If an international transfer of data is required or a research project involves an international organization, researchers must ensure compliance with relevant data protection regulations. This includes adhering to local and international data protection laws, institutional data protection policies, and other applicable legal frameworks. Researchers should secure the necessary permissions before beginning data processing, notify relevant supervisory authorities or ethics committees, and fulfill any additional legal obligations imposed on them.[9]

A researcher is also responsible for maintaining data accuracy and updating it periodically. Data security measures must be upheld, and the rights of data subjects—such as the right to erasure, also known as the "right to be forgotten"—must be protected. Personal data should be stored in a way that prevents subject identification and should not be retained longer than

[6] Ibid, 3 (f).

[7] *Schaar K.,* Working Paper: What is important for Data Protection in science in the future? General and Specific Changes in Data Protection for Scientific Use Resulting from the EU General Data Protection Regulation RatSWD Working Paper, No. 258, 2016, 6.

[8] *Chassang G.,* The Impact of the EU General Data Protection Regulation on Scientific Research, Ecancer Medical Science, 2017, <https://pubmed.ncbi.nlm.nih.gov/28144283/> [20.02.2025].

[9] Recommendations of the Personal Data Protection Service on the Development of a Privacy Policy Document, 2025, 11.

necessary for the intended research purpose.[10] While access to data may be required for reporting purposes after a study's completion, indefinite data storage is not considered an acceptable practice.[11]

To ensure compliance, it is crucial to establish a clear data retention and deletion plan at the outset of the study. If necessary, an automated data deletion function should be implemented. The retention period of personal data should align with the original purpose of collection or any justified re-processing needs. Once data is no longer necessary for the research, it should be deleted or archived in a depersonalized form.[12]

Internationally, the burden of proving compliance with data protection principles rests with researchers, research project leaders, and institutions. For example, the UK's Information Commissioner's Office (ICO) imposed an administrative fine on the University of Greenwich for a personal data security breach linked to a student-led research project.[13] The breach occurred because the student failed to implement proper security measures for a research-related website, allowing hackers to access the personal data of 20,000 individuals, including special category data subjects. This case underscores the importance of conducting thorough risk assessments, enforcing data security policies, and maintaining strict compliance controls for personal data processing.

The processing of special categories of personal data for academic research purposes is generally based on the explicit consent of the data subject. These special categories include, among others, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and information related to health, sexual orientation, or sexual activity.[14] When processing such sensitive data, researchers must submit a valid legal basis for processing to the relevant ethics committee. It is essential to justify the necessity of data collection within the research framework and assess the proportionality of data processing to ensure compliance with legal and ethical standards. Additionally, personal data collected from different sources may only be combined if explicitly permitted by law.

[10] EDPS, Preliminary Opinion on Data Protection and Scientific Research, 2020, 23.
[11] ICO, Guideline on Principle of Storage Limitation, <https://ico.org.uk/> [20.02.2025].
[12] European University Institute, Guide on Good Data Protection Practice in Research, 2022.
[13] MDPI and ACS Style, *Lallie H. S., Thompson A., Titis E., Stephens P.,* Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector, 2025, 20.
[14] Article 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).

3. Obtaining Informed Consent for Personal Data Processing

For data processing to be lawful, the data subject's consent is generally required. However, processing personal data without consent is permissible in exceptional cases, such as when the processing does not adversely affect the legitimate interests of the individual, the public interest in conducting the research outweighs the data subject's rights, or the research objectives cannot be achieved otherwise or would require disproportionate effort. The lawfulness of processing without consent often depends on balancing the right to confidentiality with the potential benefits of the research.[15] In some situations, under fundamental regulations, processing may be permitted without specifying the exact purpose[16]—such as during a public health emergency—provided that ethical research standards are upheld.[17]

The data subject has the right to withdraw consent at any time without providing a reason. They also have the right to request the erasure or blocking of their processed information.[18] If a researcher fails to obtain valid consent, they may face legal challenges or liability. "Valid" consent must be freely given, without coercion, intimidation, or misleading information. It must be specific, clearly defined in relation to the purpose and scope of data processing. It must also be informed, meaning the data subject must understand what information is being processed and why, and unambiguously, demonstrated through an explicit and affirmative act.[19]

A valid consent process ensures that data subjects have a genuine choice regarding the collection and use of their data. It is not sufficient if consent is influenced by any form of pressure or manipulation[20]. The respondent's consent needs to be specific, clearly identified, accurately respond to, and agree with the purpose and results of the data processing.[21]

[15] *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021, 26.
[16] *Malgieri G.,* Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic, Computer Law & Security Review, 2020, 3.
[17] Recital 33, 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).
[18] Guideline 05/2020 on consent, under Regulation 2016/679, 9.
[19] Recital 32, 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).
[20] EDPS, A Preliminary Opinion on Data Protection and Scientific Research, 2020, 19.
[21] Guideline 05/2020 on consent, under Regulation 2016/679, 21.

In some cases, a single consent may cover multiple processing operations if the data subject, based on the provided information, can reasonably anticipate how their data will be used. Research participants must receive comprehensive and accurate information regarding the purpose of data processing, the categories of data being processed, the duration of data processing and storage, any secondary data processing or transfers, and their rights as data subjects, including the right to object to data processing.[22]

Research participants must receive comprehensive and accurate information regarding the purpose of data processing, the categories of data being processed, the duration of data processing and storage, any secondary data processing or transfers, and their rights as data subjects, including the right to object to data processing.[23]

The data controller bears the responsibility of proving that valid consent has been obtained for a specific research purpose.[24] Several factors should be considered in this regard, including the relationship between the researcher and the data subject, such as whether there is a power imbalance or dependency, any economic or legal influence on the data subject, as well as the vulnerability of the research participant and the potential impact of the research on them or society.

4. "Secondary Processing" of Personal Data

When personal data is processed again for a purpose different from its original intent, it constitutes secondary data processing. Such processing is unlawful if data collected for one research project is used for another without the data subject's knowledge and consent.[25] However, it is lawful if the data subject's initial consent explicitly includes permission for further processing in new research or if researchers obtain fresh consent for the new study.[26]

Researchers are responsible for fully informing data subjects when collecting personal information, emphasizing the importance of informed consent. Additionally, if publicly available data is used, it is advisable to cite the

[22] WP29 Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251), point IV.B, pages 20 et seq.

[23] See also GDPR Preamble, paragraph 42: "[...] In order for consent to be informed, the data subject must be informed, at least, of the identity of the controller and the purposes of the processing. [...]."

[24] Article 7 and Recital 32, 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).

[25] Ibid, Recital 50.

[26] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 7.

source. Throughout the research process, correctly identifying and adequately protecting personal data categories is essential. Personal data may include a subject's name, home address, email address, or geographic location, while special categories—such as religious beliefs, political opinions, or medical data—require heightened protection due to the potential harm that unauthorized disclosure may cause.[27]

The selection of technical and organizational measures for data protection should consider the identity of the respondents, as different categories of data subjects may require tailored safeguards. Research participants may include patients, volunteers in surveys or medical studies, employees (e.g., laboratory staff), fellow researchers, minors, or adolescents, each necessitating varying levels of data protection.[28]

When secondary processing is not based on consent or a legal requirement, the controller may still process data in line with the original purpose if a "compatibility test" is satisfied.[29] This test assesses whether the new purpose aligns with the initial one, taking into account factors such as the relationship between the original and new purposes, the context in which the data was collected, the sensitivity of the data, the impact on the data subjects' rights, and whether adequate safeguards[30] mitigate the risks of processing.[31]

Article 4 of the Law of Georgia on Personal Data Protection outlines exceptions where further data processing is deemed compatible with the original purpose. These exceptions include processing for archiving, scientific, historical research, or statistical purposes[32] in the public interest. However, even in such cases, controllers must evaluate the lawfulness of further processing, particularly by assessing its compatibility with the initial purpose of data collection

[27] Personal Data Protection Service, Personal Data Protection Guidelines and Recommendations for Small and Medium-Sized Entrepreneurs, 2024, 11.
[28] Recommendations of the Personal Data Protection Service on the Principles of Personal Data Processing, 2024, 17.
[29] *Mészáros J., Ho Chih-hsing,* Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, 2018, 4.
[30] Art. 89, 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).
[31] Ibid, art. 5(1).
[32] Recommendations of the Personal Data Protection Service "On the Principles of Personal Data Processing", 2024, 17.

5. Key Considerations During the Planning and Implementation Stages of Research

To comply with data protection legislation, researchers must carefully consider the information provided to study participants. This information should be presented in clear and accessible language, ensuring that respondents can make an informed and voluntary decision about their participation. One effective way to inform participants is by providing a pre-prepared information sheet[33] about the study, along with an informed consent protocol attached to the questionnaire.[34]

A crucial aspect of informing respondents about data processing is establishing initial contact and inviting them to participate. Even when respondents are family members or friends, it remains essential to share all relevant information and obtain explicit consent for data processing. If a person cannot provide consent—such as in the case of minors—permission must be obtained from their parent, guardian, or legal representative.

For research involving fieldwork, obtaining informed consent may be an ongoing process rather than a one-time procedure. The process may evolve as new, unforeseen issues arise during the study. In such cases, researchers may need to renegotiate consent, especially if additional information is required during an interview or questionnaire. At the outset of communication, respondents should also be informed about possible exceptions to obtaining informed consent and the potential need for renegotiation, depending on the conversation's direction or the study's evolving needs.

Cultural and ethical norms must be taken into account when obtaining consent. In some communities, written consent may not align with local ethical standards, or it may be impractical to obtain. In such cases, alternative consent mechanisms—such as verbal consent records or the presence of a witness—should be considered. Regardless of the method used, proper documentation of the consent procedure must be maintained. When respondents cannot clearly express their wishes or fully comprehend the information, informed consent should be replaced with an appropriate alternative measure.

For observational research, consent must be obtained from both data subjects and any responsible supervisors, guardians, or authorities before the study begins. However, observations conducted in public spaces may not

[33] *Katulic T., Katulic A.,* GDPR and the Reuse of Personal Data in Scientific Research, International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, 1311-1316.
[34] European University Institute, Guide on Good Data Protection Practice in Research, 2022, 15.

always require consent. In these cases, researchers must ensure that their study does not alter people's behavior or infringe upon their privacy rights.[35]

Special considerations apply when conducting research involving children. Researchers should use child-friendly methods to explain data processing, such as audio or video materials or simplified information leaflets. Additionally, researchers must have the authority to process personal data. If reprocessing data initially collected for another study, new consent must be obtained unless the original consent explicitly covers further processing. When using a database created for a previous project, researchers must assess whether the initial informed consent applies to the new study. Ethical committees, data protection officers, or supervisory authorities should be consulted for guidance on these matters.

6. Data Security

To ensure the secure processing of personal data, it is essential to implement appropriate technical and organizational measures to prevent unauthorized access.[36] In academic and scientific research, one effective method for safeguarding data security is maintaining access records, known as "logging," which track who accessed specific information, when, and what data was accessed. Additional security measures may be applied based on the research context, such as user authentication, password protection for electronic files, or encrypting databases—storing data in a form that is unreadable without a decryption key.

Regardless of where data is stored—whether on a personal computer, memory card, or cloud platform—the same legal requirements for data protection apply. Clear and periodically updated rules for secure access to personal data should be in place, proportional to the level of risk and the category of data being processed. For instance, special categories of data or research involving vulnerable respondents may require stricter security measures. It is advisable to document access rules and security protocols, including encryption, password protection, and other safeguards. In some cases, data should be separated from other information to enhance security. For example, segregating databases can prevent unauthorized individuals from

[35] Ibid.
[36] EDPS, Preliminary Opinion on Data Protection and Scientific Research, 2020, 24.

identifying data subjects, and special categories of personal data may be stored separately for added protection. Additionally, an action plan may be required for handling unplanned data that researchers unexpectedly acquire during the study.[37]

To protect against unauthorized access, it may be necessary to separate personal data from other information. One effective method is the partitioning of databases, ensuring that unauthorized individuals cannot identify data subjects. Special categories of personal data may require additional safeguards, such as separate storage from general personal data. Additionally, researchers should develop an action plan for handling data that was not originally intended to be collected but became available unexpectedly during the research process.

When transferring data, the data controller must assess the adequacy of the recipient's data protection measures. Research participants should be informed if their data will be transferred to third countries. While the data controller may verbally explain international data transfers to the data subject, this can make it difficult to document consent. Therefore, it is advisable to obtain written consent reflecting the respondent's agreement to the processing of their personal data. Before transferring data abroad, the adequacy of data protection in the recipient country should be evaluated, considering the methods of transfer.[38] The Personal Data Protection Service assesses whether appropriate safeguards exist in the receiving country or international organization based on an analysis of relevant legislation and practices.[39]

Depersonalization is an effective tool for protecting personal data security, as it enables research while preserving confidentiality.[40] This process involves removing direct identifiers, such as names, birthdates, or addresses. However, it does not entirely eliminate the risk of re-identification, as data subjects may still be identifiable through the combination of different data points.[41]

A commonly used depersonalization technique is randomization, which removes any direct link between the data subject and the information.[42] If data

[37] Article 4(13), (14) and (15) andArticle 9 and Recitals (51) to (56), 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).

[38] *Tsagareishvili N.,* Legal Regulation of International Transfer of Personal Data (International and National Standards), Journal of Personal Data Protection Law, №1, 2024, 84.

[39] Law of Georgia "On Personal Data Protection", Article 42.

[40] Recommendations on the principles of personal data processing, 2024, 27.

[41] Ibid, Article 3(c).

[42] AEPD, 10 Misunderstandings relating to Anonymisation, 2021, 5.

is presented in a sufficiently vague manner, it becomes difficult to associate it with an individual.[43] Another approach is generalization, which reduces the likelihood of identification by broadening data categories. For example, instead of specifying a city of residence, the researcher may indicate only a broader region, or instead of listing a respondent's exact age, they may categorize them into an age group. However, these methods alone may not fully prevent re-identification, making it essential to choose data protection strategies tailored to the specific research context.

Adhering to the principles of data minimization and security is a crucial aspect of research ethics. A notable example is the Swedish Data Protection Supervisory Authority's decision to fine Umeå University for storing special categories of personal data on a cloud platform without implementing adequate security measures. This case underscores researchers' obligation to ensure proper data protection mechanisms, such as encryption or anonymization, when handling sensitive personal data.[44]

Another effective security measure is pseudonymization,[45] where personally identifiable characteristics are replaced with coded identifiers. If personal data is stored by a third party or in a cloud system, it is necessary to verify that the data has been securely deleted after use.[46] Additionally, when personal data is transferred to a third party, it is recommended to confirm that they have erased the information once the processing purpose has been fulfilled.

[43] Article 29 WP Opinion on Anonymisation Techniques, 2014.
[44] Decision of the DPA (Sweden), DI-2019-9432, 2020, <https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-9432> [24.02.2025].
[45] *Manis M. L.,* The Processing of Personal Data in the Context of Scientific Research, The New Regime under the EU-GDPR, BioLaw Journal, 3/2017, 344.
[46] EDPB Guidelines 01/2025 on Pseudonymisation, 2025, 36.

7. Conclusion

With the enactment of the new Law on Personal Data Protection, maintaining high standards of data security while balancing research interests has become increasingly important. Researchers now bear the burden of demonstrating compliance with data protection laws at every stage of research planning and implementation.

Respecting the confidentiality of data subjects and obtaining informed consent are fundamental aspects of the research process. In academic and scientific research, secondary data processing—where data is used for purposes beyond those originally specified—is common. In such cases, researchers must either obtain new consent from the data subject or ensure a valid legal basis for processing.

Personal data must be processed in accordance with core data protection principles: it must be handled lawfully and transparently, collected for specific, explicit, and legitimate purposes, and maintained accurately and up to date where necessary. Data should only be retained for as long as required for the intended purpose, and appropriate technical and organizational measures must be implemented to safeguard its security. Special categories of data, such as health-related or religious information, require heightened caution and explicit consent from the data subject.

Ensuring data security requires both technical and organizational safeguards, including encryption, password protection, and controlled access. Additionally, depersonalizing or pseudonymizing data can help minimize the risk of identifying individuals.

Adhering to personal data protection principles in scientific and academic research is not merely a legal obligation but also an ethical responsibility. Upholding these standards safeguards the rights of data subjects and reinforces the integrity and credibility of research.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 14/06/2023.
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 Aata, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4/5/2016.
3. *Chassang G.,* The Impact of the EU General Data Protection Regulation on Scientific Research, Ecancer Medical Science, 2017, <https://pubmed.ncbi.nlm.nih.gov/28144283/> [20.02.2025].
4. *Ducato R.,* Data protection, Scientific Research, and the Role of Information, Computer Law & Security Review, Vol. 37, 2020.
5. EDPB Guidelines 01/2025 on Pseudonymisation, 2025.
6. EDPS, Preliminary Opinion on Data Protection and Scientific Research, 2020.
7. European University Institute, Guide on Good Data Protection Practice in Research, 2022.
8. Guideline Recommendation 05/2020 on Consent, under Regulation 2016/679.
9. ICO, Guideline on Principle of Storage Limitation, <https://ico.org.uk/> [20.02.2025].
10. *Katulic T., Katulic A.,* GDPR and the Reuse of Personal Data in Scientific Research, International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018.
11. *Lallie H. S., Thompson A., Titis E., Stephens P.,* Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector, 2025, 20.
12. *Manis M. L.,* The Processing of Personal Data in the Context of Scientific Research, The New Regime under the EU-GDPR, BioLaw Journal, 3/2017.
13. *Malgieri G.,* Data Protection and Research: A Vital Challenge in the Era of COVID-19 Pandemic, Computer Law & Security Review, 2020.
14. *Mészáros J., Ho Chih-hsing,* Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR, 2018.
15. Personal Data Protection Service, Recommendations on the Principles of Personal Data Processing, 2024, 7.
16. Personal Data Protection Office, Personal Data Protection Guidelines for Small and Medium-sized Enterprises, 2024, 11.

17. Personal Data Protection Service of Georgia, Recommendations on the Development of a Privacy Policy Document, 2025.
18. *Sold M., Junk J.,* Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities, 2021.
19. *Schaar K.,* Working Paper: What is important for Data Protection in science in the future? General and Specific Changes in Data Protection for Scientific Use Resulting from the EU General Data Protection Regulation RatSWD Working Paper, No. 258, 2016.
20. *Tsagareishvili N.,* Legal Regulation of International Transfers of Personal Data (International and National Standards), Journal of Personal Data Protection Law, №1, 2024.
21. Working Party 29 Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251).
22. Decision of the DPA (Sweden), 2020, <https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-9432> [24.02.2025].

PERSONAL DATA
PROTECTION SERVICE

Address: №7 Nato Vachnadze, Tbilisi, 0105
Batumi, Baku street №48, 6010
www.pdps.ge
Tel.: (+995 32) 242 1000
E-mail: office@pdps.ge