Giuseppe D'Acquisto*

Ludovica De Benedetti**

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

1. The Concept of Data Sharing

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Legal Instruments Promoting Data Sharing

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. The Legal Architecture of Data Sharing

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Data Protection Risks in Data Sharing

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

6. Recommendations

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

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

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

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

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

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

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

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

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

6.1. Recommendations for Controllers

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

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

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

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

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

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

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

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

6.2. Recommendations for Lawmakers and Governments

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

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

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

---

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

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

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

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

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

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

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

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

6.3. Recommendations for Technology and Solution Providers

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

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

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

6.4. Recommendations for the Research Community

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

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

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

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

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

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

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

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

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

6.5. Recommendations for Data Protection Authorities

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

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

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

7. Concluding Remarks

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

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

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

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

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

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

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

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

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

Bibliography:

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

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

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