International Working Group on
Data Protection in Technology

Working Paper on "Data Sharing"

Published 6 December 2024[1]

Table of contents

[1] *This paper was discussed at the 72nd IWGDPT Meeting on 7th – 8th December 2023 and adopted, after final discussion, at the 73rd IWGDPT Meeting on 18th – 19th June 2024. The written procedure followed after the latter meeting.*

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

1. The concept of data sharing

Data are essential assets for organizations to achieve their specific purposes and to generate direct value. For instance, data may be collected and analysed to improve customer experiences, optimize business operations, or drive innovation in the organization's interest.

However, data value can extend beyond organizations that originally collect and use them. Data can be used and combined with other data sources to generate new insights, create new products and services, and drive social and economic growth. This creates additional value from the same dataset, beyond its original purpose[2].

Based on this observation, many organizations have promoted the idea of "data sharing" as a concept or as a framework.[3] This might range from a simple data governance strategy of a single company to a legally defined framework. 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"[4]. "It includes the re-use of data based on commercial and non-

[2] 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).

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

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

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

commercial conditional data-sharing agreements, as well as open data."[5] We want to stress that data sharing typically entails transferring the data from one organization to another. In this sense, the term "data transfer" might be more suitable, at least from a technical point of view.

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 often involves the processing of personal data. And the application of data sharing per se does not yet say anything about the conformity of this processing with data protection laws.

Against this background, it is essential to consider that data sharing might entail possible adverse effects for persons impacted by the use of data (it is, among others, the issue of 'group discrimination'[6]).

[5] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en.
[6] Favaretto, M., De Clercq, E. & Elger, B.S. *Big Data and discrimination: perils, promises and solutions. A systematic review*. J Big Data **6**, 12 (2019). https://doi.org/10.1186/s40537-019-0177-4

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

At the same time, it is necessary to assess whether the data shared are personal data or not.

If personal data are shared, the strict observance of data protection principles is of paramount significance. It constitutes an essential pillar in the preservation of trust between data producers and data users, which is a precondition for the generation of significant economic value.

When processing personal data 'for the public benefit' it is indeed necessary, to ensure that the processing remains proportionate to the 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. Public consultation in the definition and implementation of the 'data sharing for public good' projects, involving all stakeholders, notably the impacted communities, is of high importance also to increase trust in the project.

The "by-design" approach[7] involves embedding data protection and ethical considerations into the design of data systems, ensuring that data is handled responsibly from the outset. By adopting this approach, organizations can enhance

[7] 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).

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

their data governance and build trust with data subjects, ultimately leading to more effective and responsible use and share of data.

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 [8]. These technologies aim to mitigate privacy risks when sharing data, even if it is sensitive or confidential.

2. Legal instruments promoting data sharing

There is a worldwide interest of legislators in data sharing, with many significant legislative initiatives aimed at regulating data sharing both in the public and in the private sectors. In 2019 the OECD had already 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 goal of facilitating data sharing within the private sector. Additionally, half of the data sharing initiatives involves the sharing of personal data[9]. In the following, we present some examples

[8] The PET guide. 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

[9] The World Economic Forum (2021), *Good Data: Sharing Data and Fostering Public Trust and Willingness*, p. 6, https://www.weforum.org/whitepapers/good-data-sharing-data-and-fostering-public-trust-and-willingness/ 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 https://www.oecd-ilibrary.org//sites/276aaca8-en/1/2/3/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

for recent initiatives that aim to govern the collection, processing, and transfer of (national) data-sets:

- The European Union has recently implemented two legislative initiatives, the European Data Governance Act[10] and the EU Data Act[11], 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)[12] 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. Sections 8 – 13 of the complementary "Data Availability and Transparency Regulations 2022" [13] list "circumstances in which (data) sharing is barred".

[10] 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

[11] 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

[12] https://www.datacommissioner.gov.au/law/dat-act - Legal-Text available at: https://www.legislation.gov.au/C2022A00011/latest/text.

[13] Legal-Text of the "Data Availability and Transparency Regulations 2022" available at: https://www.legislation.gov.au/F2022L00601/latest/text.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- The "Data Sharing Governance Framework" (2022, UK) [14] 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 to substantially advance Data Sharing and Analytics among public sector bodies of the US Federal Government. Table 1 on Page 15 of this National Strategy[15] lists technologies suitable for Privacy Preserving Data Sharing and Analytics.

3. Data protection risks in data sharing

Sharing data is not without risks. The potential value of collaboration must be weighed against its implications on privacy, data security and control of business sensitive data. There are a number of risks associated with the concept of data sharing that must be addressed to ensure that personal data are protected.

These include:

- 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',

[14] https://www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework
[15] Table 1 on Page 15 of https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

including the societal impact in terms of fostering economic inclusion and mutualization[16]) and further details (lack of transparency).

- Lack of technology and understanding to ensure data processing and handling in a fair and understandable manner (lack of fairness)
- Vague definition of the scope of the processing, and a tendency towards casual discovery rather than a more scientific approach based on hypothesis testing (lack of purpose limitation)
- Data duplication or dissemination beyond the lawful or legitimate scope of the processing (lack of storage limitation and purpose limitation)
- Data wasting, namely inefficient or unnecessary use of data, storage, or resources (lack of data minimization)
- Security incidents and data breaches, as large amounts of data are stored and transmitted across multiple networks and systems managed by different organizations with different policies (lack of confidentiality, integrity and availability)
- Reduction in data quality, which in turn can result in incorrect decisions and actions and possibly in bias or discriminations, due to the heterogeneity of data sources (lack of data accuracy and possibly fairness)
- Unlawful access, use, or disclosure, as data are shared across multiple organizations and systems, and it may be difficult to establish a consistent governance framework (lack of lawfulness)
- Difficulty in enforcing the responsibility or liability of organizations for their data processing activities, as it may be difficult to identify the relevant data protection roles when different organizations are involved in complex data processing activities (lack of accountability)

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

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Ultimately, all data protection principles are relevant to data sharing, and the only 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 permissive of data sharing. Sharing of personal data must comply with the aforesaid principles, including the principle of necessity and proportionality, which refers to 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. The assessment of the adoption of concrete measures to mitigate risks to individuals' rights and freedoms is part of this balancing test. Data protection laws are enablers of data sharing since they provide a framework for carrying out such practices in a compliant way with these fundamental rights.

4. Data sharing paradigms with data protection safeguards

Data sharing is not an unregulated option for personal data processing. It must be respectful of data protection principles and individuals' rights. This entails a number of requirements for data controllers, such as:

- Establishing consistent and robust data governance frameworks to ensure that personal data is managed in a responsible and ethical manner
- Conducting a thorough risk assessment to identify potential risks associated with data sharing, also including privacy and data protection impact assessments (PIAs/DPIAs) to assess the potential privacy risks associated with data sharing and identify appropriate mitigation measures

- Implementing policies and procedures for data retention and disposal, to ensure that personal data is not retained longer than necessary and is securely disposed of when no longer needed
- Conducting regular audits and reviews of the data sharing process to ensure compliance with legal and regulatory requirements
- Enhancing transparency, notifying individuals whose personal data is being shared and providing them with information about their rights, including the right to access and correct their personal data
- Improving the accuracy and quality of data, through controls including data validation, or age verification where needed
- Conducting necessity and proportionality tests, in order to minimize the amount of personal data transferred to other organizations, thereby reducing the risk of data breaches and privacy violations
- Implementing procedures for preventing and responding to data breaches and other security incidents, as well as mitigating the impact on individuals
- Implementing multilateral data sharing agreement that clearly defines the purpose, scope, and terms of the data sharing, including limitations on use of shared data, confidentiality obligations and prohibition of re-identification attempts without a legal basis, training to employees to ensure that they are aware of the risks associated with data sharing and are equipped with the knowledge and skills to manage these risks effectively
- Implementing data portability mechanisms empowering data subjects to receive the personal data concerning him or her in a structured, commonly used and machine-readable format or transmit those data to another controller.

In addition to these organizational aspects, 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

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

reducing – the risks historically associated with collaboration in many practical use cases. Most PETs are mature enough to enable the exploration of previously unimaginable opportunities.

Traditional collaboration paradigms involve merging local datasets into a single dataset accessible by all participants. Today, technologies allow going beyond this naïve vision of data sharing, offering the possibility to carry out computations, or other logical operations at the core of data processing, minimising the amount of personal data required to be shared, and to protect the data used in computations against undesired inference made on their results. PETs can assist with both input and output privacy.

Among PETs for input privacy one can enumerate private set intersection, homomorphic encryption, secure multiparty computation and zero knowledge proofs. Instead, the output privacy problem can be tackled with two additional PETs: randomization (as in differential privacy) and generalization (as in k-anonymity).

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.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

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[17].

One instance of input privacy is the reconciliation of trade data across international borders. Import data compiled by one country can be compared with the export data of the partner country using multiparty computation techniques such as private-set intersection. Whereas neither country is allowed to show transaction-level trade information, it is still possible to exchange coherent information. Input privacy techniques such as secure-multiparty computation can be used as an advanced form of pseudonymisation when the inputs are personal data[18].

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[19]. In legal terms, these output privacy techniques might be regarded as anonymization techniques.

[17] 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.
[18] ENISA Data Pseudonymisation: Advanced Techniques & Use Cases Technical analysis of cybersecurity measures in data protection and privacy - January 2021
[19] 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

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

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[20].

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.

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.

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

[20] 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

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

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[21] and the use of synthetic data[22].

5. 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[23].

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

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

[23] Citron, Danielle Keats and Solove, Daniel 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), Available at SSRN: https://ssrn.com/abstract=3782222 or http://dx.doi.org/10.2139/ssrn.3782222

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

These risks require the implementation of a variety of measures and approaches, both technical and legal, to evaluate and mitigate privacy risks comprehensively and 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 unimaginable opportunities for collaboration can now be explored, while upholding

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

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"[24].

6. Summary of recommendations

When two or more organizations opt to collaborate and share their data, they become part of a broader and richer data ecosystem within which they can uncover, by way of computations, new insights or trends regarding individuals, groups, or society as a whole. The approach of directly and bilaterally exchanging raw data, or merging them into a shared database accessible by all parties is inappropriate and difficult to enforce, especially when the parties are distributed and volumes grow. It is necessary to implement a multilateral approach, based on

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

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

the widespread use of PETs, in which the stakeholders contribute to the development of a trusted sharing and computational environment, which can maximize the potential of secure and safe data exchange while preserving data protection principles.

In this respect, the International Working Group on Data Protection in Technology identifies a number of key actors to whom the following recommendations are addressed.

6.1 Recommendations for controllers

Controllers should consider in the first place why they are sharing data, who they are sharing data with and whether this has been adequately communicated to individuals to whom the data relates. It is important that these individuals are provided by the controller with clear and easily accessible information before the data processing (collection and sharing of personal data). The information must not be hidden in endlessly long terms, but come across clearly, in short and clear text. This can be clickable for those who want further information. It must also be possible to object to against such sharing.

When personal data are shared, this is or entails processing of personal data. This triggers obligations for organizations sharing data and implies responsible data handling. All the relevant steps should be done to ensure compliance with the applicable data protection laws in any jurisdiction where the sharing takes place, starting from the selection of the proper legal basis for sharing data. A list of more detailed recommendations on the organizational aspects of ensuring compliance with data protection principles can be found at the beginning of chapter 4.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Using PETs can help mitigate the risk of sharing of personal data, particularly for higher risk data, e.g. special categories of personal data, and they might allow, under assumptions and circumstances depending on the specific jurisdiction, international data transfer that may otherwise not be possible. Organizations should be aware of the business enabling opportunities offered by the use of PETs, and should consider their adoption carefully and consciously.

6.2 Recommendations for Lawmakers and Governments

Lawmakers and governments should develop a comprehensive vision for data sharing that extends beyond simple data handovers between organizations, limiting data concentrations and excessive data centralization.

They should also assess the wider social and economic implications of data sharing and the role of PETs in mitigating novel risks, including how PETs might positively open digital markets to competition.

Legislative initiatives should aim at establishing legal frameworks that promote the use of PETs for data protection, encouraging organizations to transition to more privacy-friendly technologies. Institutions should invest heavily in researches aimed at making these techniques easier to use in real-life applications. Governments should incentivise the use of PETs, for example by making them affordable by adequate, targeted subsidies.

Data strategies, at any level, developed by governments should prioritize compliance with data protection regulations and the creation of a robust computing infrastructure with embedded and enforceable rules. In this regard,

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

public-private partnerships and the creation of sandboxes for collaborative experimentation can build trust among stakeholders and foster innovation while maintaining high standards of privacy.

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. 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.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

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.

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.

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-proposed technologies and approaches meet the required standards of security and privacy.

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.

Data Protection Authorities should encourage organizations to align the perceived value of data protection with their actual implementation, and facilitate

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

collaboration and communication between data protection experts and technologists to bridge the existing knowledge gap on PETs.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology