Deloitte.
Legal

Data Protection | E-book
Privacy Enhancing Technologies (PETs)
EU and UK overview

MAKING AN IMPACT THAT MATTERS since 1845

October 2023

Index

1. Legal underpinning to PETs

In recent years, there has been increased development and market release of **new technological solutions** and **applications** that involve **complex processing operations**, including the **growing use of artificial intelligence** (AI) systems. This trend has resulted in **increased privacy threats** and **risks for data subjects**, such as the processing of large amounts of data, the lack of control over data, the re-use of data for different purposes, intrusive profiling activities, automated decision making, etc.

Within this context, it is more important than ever that organisations **minimise privacy risks** by **designing processing operations that respect the rights and freedoms of data subjects** in relation to the processing of their personal data.

The requirement for organisations to minimise privacy risks is underpinned by several legal obligations in the GDPR:

- **Article 25**, which requires organisations to implement **appropriate technical and organisational measures** to effectively implement the data protection principles (also known as the privacy by design and default principles).

- **Article 5**, which includes the data protection principles referenced in Article 25:
  - lawfulness, fairness and transparency;
  - purpose limitation;
  - data minimisation;
  - accuracy;
  - storage limitation;
  - integrity and confidentiality; and
  - accountability.

- **Article 32,** which requires organisations to implement appropriate technical and organisational measures to **ensure a level of security appropriate to the risk**, including, as appropriate, the pseudonymization and encryption of personal data.

*When used in this publication, the term “GDPR” is used to mean both the EU GDPR and the UK GDPR.

2. Introduction to PETs

A key method that regulators are increasingly recommending to support compliance with the legal requirements under Articles 25, 5, and 32 of the GDPR is via the use of **privacy enhancing technologies** ("**PETs**"). Most recently:

- the **UK Information Commissioner's Office** (**ICO**) released guidance on privacy-enhancing technologies in June 2023; and
- the **European Union Agency for Cybersecurity** (**ENISA**) released a reported on "*Data Protection Engineering*" in January 2023.

PETs are defined by the ENISA as **software and hardware solutions**, i.e., **systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons**.

Practically, different PETs will facilitate compliance with different data protection principles based on their **particular functionality or purpose**. For example, some PETs have the effect of **minimising the amount of data** shared, while others seek to **preserve the accuracy of data** or the **confidentiality of data** through the application of technical measures such as encryption or pseudonimisation.

This publication is intended to provide you with an overview of the recent ICO guidance and ENISA report, and briefly highlight some other key regulatory guidelines relating to PETs. This publication will also cover a handful of example regulatory decisions and court cases where the use of PETs could have remedied deficiencies in an organisation's data processing practices. Finally, we will zoom in on an example PET use case: the use of synthetic data.

3. Recent PET guidance: UK ICO

The UK ICO published its finalised guidance on "*Privacy-enhancing technologies (PETs)*" in June 2023 ("**ICO Guidance**"). The ICO Guidance addresses the use of PETs within the context of the UK GDPR. Although a different law, the UK GDPR currently mirrors the legal requirements of the EU GDPR which can give rise to the need for PETs:

1. the privacy by design and default principles;
2. the data protection principles; and
3. the requirement to implement appropriate organisational and technical measures.

The ICO Guidance emphasises that the use of PETs can result not only in better protection of personal data, but can also serve to unlock the true value of data and drive innovation. John Edwards, the UK Information Commissioner, said "*By enabling organisations to share and collaboratively analyse sensitive data in a privacy-preserving manner, PETs open up unprecedented opportunities to harness the power of data through innovative and trustworthy applications.*"

The first section of the ICO Guidance is aimed at individuals with data protection compliance responsibilities. In addition to addressing how PETs can facilitate data protection compliance, key points include:

- PETs are likely to be most appropriate in the context of processing of **large datasets** (especially **special category data**), where a **data protection impact assessment** has identified risk areas that capable of being mitigated by PETs and, especially, in the **finance, healthcare, research, and government sectors.**
- PETs will not always be appropriate and if not **properly implemented**, can be counterproductive to privacy efforts. Some PETs may also not be sufficiently **mature** for certain purposes, and the ICO Guidance includes information on relevant **standards** and known **weaknesses** in relation to specific PETs.
- There are different ways of categorising PETs, for example by viewing PETs as providing **input privacy** (PETs that reduce the number of parties with access to the personal data) or providing **output privacy** (PETs that reduce the risk that people can obtain or infer personal data from the result of the activity).

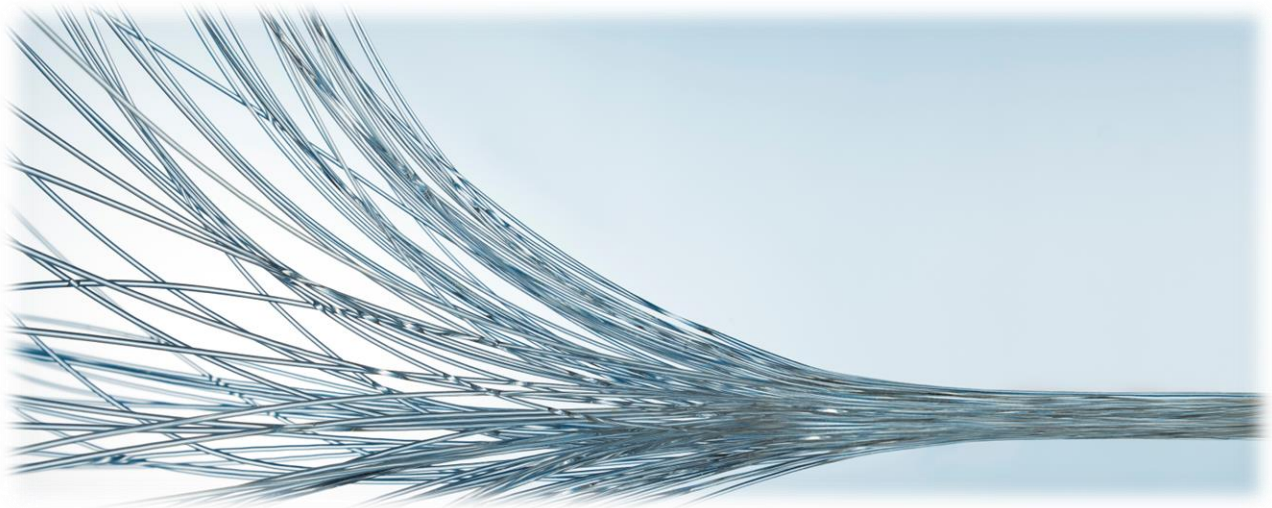
3. Recent PET guidance: UK ICO

The second section of the ICO Guidance is aimed at individuals who may be responsible for the technical implementation of PETs. It provides information on a number of key PETs, including:

- **Differential privacy:** generates anonymous statistics, usually by randomising the computation process that adds noise to the output.
- **Synthetic data:** provides realistic datasets in environments where access to large real datasets is not possible.
- **Homomorphic encryption:** provides strong security and confidentiality by enabling computations on encrypted data without first decrypting it.
- **Zero-knowledge proofs (ZKP):** provide data minimisation by enabling parties to prove private information about themselves without revealing what it actually is.
- **Trusted execution environments:** enhance security by enabling processing by a secure part of a computer processor that is isolated from the main operating system and other applications.
- **Secure multiparty computation (SMPC):** provides data minimisation and security by allowing different parties to jointly perform processing on their combined information, without sharing all information with each other.
- **Federated learning:** trains machine learning models in distributed settings while minimising the amount of personal information shared with each party, usually in combination with other PETs.

The ICO Guidance links to a number of practical resources, including the UK Centre for Data Ethics and Innovation's interactive tool designed to aid decision-making around the use of PETs in data-driven projects.

The ICO Guidance is a valuable resource for any organisation considering the implementation of PETs, which the ICO recommends organisations should consider doing within the next 5 years in relation to data-driven activities.



4. Recent PET guidance: EU ENISA

In 2022, the European Union Agency for Cybersecurity ("**ENISA**") published a Report entitled "Data Protection Engineering" where it found that "*Data Protection Engineering can be perceived as **part of data protection by design and by default**. It aims to support the selection, deployment and configuration of appropriate technical and organizational measures in order to satisfy specific data protection principles*".

Based on the characteristics of the technology used in relation to the personal data being processed, a possible categorization that ENISA has made is the following:

- **Truth-preserving**: preservation of the accuracy of data while reducing their identification power, for example diluting the granularity of data (e.g. from date of birth to age);
- **Intelligibility-preserving**: keeping personal data in a format which "has a meaning" for the data controller, without revealing the real attributes of data subjects;
- **Operable Technology**: math and logic operations on encrypted data without understanding the actual data itself.

Some of other available techniques mentioned to practically implement data protection principles are: (i) **anonymisation and pseudonymization**, (ii) **techniques beyond encryption in the areas of data masking and privacy preserving computations**, (iii) **technologies on privacy preserving access control, storage and communications**, (iv) **technical measures in the area of transparency, intervenability and user control tools**.

In addition to the information provided about data protection engineering, the ENISA focuses its attention on **how data subjects can independently exercise their data protection rights**. This is strictly related to data protection and privacy by design and by default principles. According to ENISA, this implies both access to information on data processing (transparency) and the ability to influence processing of their data within the realm of a data controller or data processor (intervenability). In this context, data controller/processor are encouraged to make privacy policy more comprehensible by adding graphical symbols (icons) and to create privacy dashboards that can provide data subjects with a general overview on how personal data is being processed.

The fundamental role played by PETs in data protection and the need for companies to implement them in their data management system also arisen during the Roundtable of **G7 Data Protection and Privacy Authorities** of last year, where discussions were made about the current regulatory and technological issues in the context of "*Data Free Flow with Trust*". In that occasion, the Authorities pointed out that the use of PETs **can help companies to improve data protection by design** (e.g. using processing capable of transforming personal to reduce its identifiability), and that **it is necessary to promote the use of these technologies to facilitate data sharing**, also in the context of international data transfers, by implementing appropriate security measures.

5. Other key guidance

Over the years, several bodies and authorities have published **guidelines and reports** related to the proper use of PETs.

Already in 2007 the Italian Data Protection Authority ("**Garante**") has emphasized in its "***Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context***" the **importance and the burden on data controllers to adopt PETs in order to minimize the use of identification data** processed through Internet and e-mail in the workplace.

In 2017, the Office of the Privacy Commissioner of Canada ("**OPC**") published a report named "***Privacy Enhancing Technologies – A Review of Tools and Techniques***" where it outlined the gaps between the risks that the ongoing evolution of technologies raises for the rights and freedoms of data subjects (e.g. risks of identity disclosure, linking data traffic with identity, etc.) and the importance of implementing PETs to lower such risks.

In 2021, the OPC published the blog "***Privacy Tech-Know blog: Privacy Enhancing Technologies for Businesses***" focused on the technical developments of PETs, to support businesses for better data privacy. It focused also on the following concepts:

- **federated learning**: a machine learning approach that allows multiple devices or parties to collaboratively train a shared machine learning model while keeping their data decentralized and private;
- **differential privacy**: technology that protects data about individuals in a dataset but allows larger statistical trends in the dataset to be studied. This is possible adding a mathematically defined amount of "noise" - or fake data - to a dataset. It can be used, for instance, to obtain relevant information for profiling activities or to predict general trends and purchases, without impacting specific data subjects.

In 2019, the Agencia española proteciòn datos ("**AEPD**") published "A Guide to Privacy by Design" where it pointed out that ensuring privacy and establishing a framework to protect personal data **offers several advantages and opportunities** for:

- ❑ **organizations**: to improve efficiency, optimize processes, establish a cost-reduction strategy and gain a competitive edge;
- ❑ **market**: to develop long-term sustainable economic models;
- ❑ **society**: to have access to the benefits of technological advances without compromising personal freedom and independence.

The AEPD's Guide classifies PETs also on the basis of their technical characteristics and on the goals that they pursue. A categorization proposed is the following:

- ❑ **privacy protection**: this type of category uses the combination of tools that actively protect privacy during the processing of personal data (e.g. pseudonymization, anonymization and encryption tools, tools, filters and blockers, anti-trackers, etc.);
- ❑ **privacy management**: technologies that support privacy management processes without actively processing personal data (e.g. information and administrative tools to manage user identity and permissions, etc.).

6. Relevant case law and regulatory decisions

Italy

The Garante considers these types of technologies necessary to process personal data in compliance with data protection principles.

In the ***Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context*** of 2007 the Garante provided rules and recommendations for employers to lawfully process personal data, with specific regard to the use of e-mail and the Internet in the workplace.

In particular, the **employer has the duty to put in place all the technological measures to minimise the use of personal data collected during the performance of the working activities through e-mail and internet, such as implementing the use of PETs**. The measures to be adopted may be differentiated according to the technology used.

In addiction, the Garante issued over the last years the following relevant decisions concerning PETs.

- ✓ In the Decision dated 13 May 2021, the Garante found that data controller carried out preventive and generalized collection of data related to the Internet browsing history of employees, which they were retained for thirty days with the possibility to extract reports related to individual employees for the purpose of protecting the security of the system and of the network, performing a processing not necessary and proportionate.

  Data controller had implemented a system that replaced the userIDs (contained in the log files and originally consisted of the first name last name) with a machine ID. The machine ID would have permitted to recall the specific user only by matching it with further information that contained the match of each user to a specific machine ID. The Authority ruled that **merely pseudonymizing the data at issue is not an adequate measure to respect data minimization.**

  The Garante found that the fact that the personal data collected were **pseudonymized, failing to ensure adequate separation between Internet browsing data** (including in particular the URL visited) **and employee identities**, constituted an infringement of the provisions that forbid to collect data relating to the personal life of employees. In this context, the Authority ordered to adopt **suitable technical and organizational measures to anonymize the data related to the employees' workstation recorded within browsing log files** (and to delete all log files already collected).

6. Relevant case law and regulatory decisions

- ✓ In the Decision dated 10 June 2021 concerning **whistleblowing**, the data controller had not implemented **encryption** for the transport and storage of data related to whistleblowing reports and the application used for the management of whistleblowing reports allowed the tracking of **accesses by data subjects** (log files included the IP of the device used), in breach of **privacy by design and default principles, the integrity and confidentiality principle, as well as art. 32 of GDPR** "**security of the processing**".

In both cases data controllers should have implemented adequate organizational and technical security measures. The use of PETs would have contributed to comply with data protection law.

Belgium and the Netherlands

Recently, also other European Data Protection Authorities and Courts have emphasized the importance of using PETs. It is worth mentioning the following decisions, both connected with promotional activities:

- ❖ In 2020, the **Belgian Autorité de protection des donneès** ("**Belgian DPA**") imposed a fine on a non-profit organisation for direct marketing practices without legal basis and notwithstanding the data subjects had repeatedly exercised the right to object. The Belgian DPA stated that a data controller who intends to use the legitimate interest as a legal basis has the obligation to provide **additional safeguards for the benefit of data subjects**. In particular, the data controller has to provide «*additional safeguards that may mitigate undesirable consequences for the data subject, such as data minimisation, **privacy enhancing technologies**, enhanced transparency, the general and unconditional right to opt-out and data portability*" (APD/GBA - 28/2020).

- ❖ In 2020, an **Amsterdam Court** found that a BigTech violated the provisions of GDPR by processing personal data for advertising purposes. The Court stated that a data controller has to balance both its legitimate interest and the interests and rights of the data subjects, listing **different safeguards to prevent undue consequences for data subjects**, such as "*extensive use of anonymization techniques, data aggregation, **privacy enhancing technologies**, privacy by design, privacy and data protection impact assessments*". (C/13/683377 / HA ZA 20-468)

7. Example PET: Synthetic data

An example PET covered by the ICO Guidance is the use of synthetic data. Synthetic data is artificial data that **replicates the patterns, properties, characteristics, and structure of the real data** on which it is based. The process of synthesising data aims to **weaken or break the connection** between real data subjects and the resulting synthetic dataset.

Synthetic data is useful for operations that **require access to large datasets containing personal data**, all or some of which does not need to be linked to real data subjects to achieve the **intended purpose**. Usually, a smaller "real" dataset will be synthetised and **extrapolated** to create a much larger dataset.

Datasets may either be partially or fully synthetised, however it is important to note that even **fully synthesised datasets may still contain personal data**. As such, **creating synthetic data is not the same as anonymising data.** In many cases, synthetic data may still be able to reidentify the original data subjects **via inference**, e.g. by combining personal data already known with observations of the inputs and outputs of an AI model.

A major challenge is to appropriately **balance the risk of reidentification with the need to still derive utility** from a synthetic dataset. A deeply synthesised dataset is likely to be more protective of privacy, but also less useful for the intended purpose, e.g. it may be stripped of outliers present in the original dataset which are needed in the synthetic dataset. However, even where synthetic data does not result in anonymisation, it can go a long way towards **facilitating compliance with the data minimisation principle.**

Another key challenge is that synthetic data will usually **carry through any biases** that are inherent in the original dataset. It is therefore important to ensure that the original dataset is **representative** of the relevant population and that any biases can be **detected and appropriately mitigated.**

Key use cases for synthetic data include the training of artificial intelligence (AI) models and research and development purposes. To zoom in on the example of **generative AI:**

- Generative AI models use **vast amounts of personal data** scraped from public internet sources to train models.
- This presents a number of **data protection compliance challenges**, such as in relation to the data minimisation and lawfulness principles, transparency obligations, and fulfilling data subject rights.
- Excluding or minimising the presence of personal data in generative AI training sets through the use of synthetic data can **significantly reduce the compliance burden, as well as the risks to individuals.**
- The use of synthetic data is therefore expected to become a **growing trend** in this space.

Experience the future of law, today

Today, you need smart lawyers who bring even more to the table than legal advice and memorandums. You need to work better, faster and with lower total cost. That takes someone who knows your business and your industry, yet thinks and works in new ways. A steady hand at the center of the transformation all around us. An expert in law, commerce and technology, who is able to serve you globally.

To make an impact that matters, you need an accomplished confidante who is both pragmatic and pioneering.

Deloitte Legal invites you to experience the future of law, today. Meet current obligations more effectively while anticipating future opportunities.

To make an impact that matters, you need an accomplished confidante who is both pragmatic and pioneering.

Deloitte Legal invites you to experience the future of law, today. Meet current obligations more effectively while anticipating future opportunities.

Automate complicated and time-consuming legal activities. Benefit from a commercial mindset that integrates legal, business and industry expertise. Draw upon our experience with business operating model transformation.

As you lead your enterprise through unprecedented complexity and change, we'll work with you not just for you. Working together, you're empowered to make confident decisions, guide your business and take advantage of possibilities.

Experience the future of law, today.

Key contacts Data Protection Teams

Ida Palombella

Partner - ipalombella@deloitte.it

Pietro Boccaccini

Director - pboccaccini@deloitte.it

Simone Prelati | Camilla Torresan

Associate

Fabris Cavan

Partner - cfabris@deloitte.co.uk

Katherine Eyres

Director - keyres@deloitte.co.uk

Shamerah Neville

Associate

Deloitte.
Legal