OECD publishing

EMERGING PRIVACY ENHANCING TECHNOLOGIES

CURRENT REGULATORY AND POLICY APPROACHES

OECD **DIGITAL ECONOMY PAPERS**

March 2023 **No. 351**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report examines privacy-enhancing technologies (PETs), which are digital solutions that allow information to be collected, processed, analysed, and shared while protecting data confidentiality and privacy. The report reviews recent technological advancements and evaluates the effectiveness of different types of PETs, as well as the challenges and opportunities they present. It also outlines current regulatory and policy approaches to PETs to help privacy enforcement authorities and policy makers better understand how they can be used to enhance privacy and data protection, and to improve overall data governance.

This report was drafted by Christian Reimsbach-Kounatze (Digital Economy Policy Division) together with an external consultant, Mr. Taylor Reynolds (Technology Policy Director of MIT's Internet Policy Research Initiative), under the supervision of Clarisse Girot (Digital Economy Policy Division).

The report is a contribution to IOR 1.3.1.2.3 of the 2021-2022 Programme of Work and Budget (PWB) of the Committee on Digital Economy Policy. It was approved and declassified by the Committee on Digital Economy Policy on 27 February 2023.

This publication is a contribution to Phase III of the OECD Going Digital project, which aims to provide policy makers with the tools they need to design and implement better data policies to promote growth and well-being.

For more information, visit www.oecd.org/going-digital.

#GoingDigital

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/2022/10/FINAL

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Table of contents

Executive summary

Overview

Privacy-enhancing technologies (PETs) are a collection of digital technologies and approaches that permit collection, processing, analysis and sharing of information while protecting the confidentiality of personal data. In particular, PETs enable a relatively high level of utility from data, while minimising the need for data collection and processing. PETs are not new but latest advances in connectivity and computation capacity have led to a fundamental shift in how data can be processed and shared. While still in their infancy, these developments hold immense potential to move society closer to the continuing process and practice of privacy by design, and thereby to foster trust in data sharing and re-use.

A growing number of policy makers and privacy enforcement authorities (PEAs) are considering how to incorporate PETs in their domestic privacy and data protection frameworks. However, the highly technical and fast evolving nature of these technologies often presents a barrier to implementation by organisations and to their consideration in policy and legal frameworks applicable to data.

This report, informed by a questionnaire to OECD members and partner economies on their regulatory and policy approaches to PETs, aims to help policy makers and regulators, most notably PEAs, better consider PETs for privacy protection, and data governance more broadly. To that end, it takes stock of technological developments related to PETs; assesses the maturity of various types of PETs and the opportunities and challenges of their use; and presents current regulatory and policy approaches to PETs.

Key technologies, their maturity, opportunities and challenges

PETs can be divided into four categories: data obfuscation, encrypted data processing, federated and distributed analytics and data accountability tools

- **Data obfuscation tools** include zero-knowledge proofs (ZKP), differential privacy, synthetic data, and anonymisation and pseudonymisation tools. These tools increase privacy protections by altering the data, by adding “noise” or by removing identifying details. Obfuscating data enables privacy-preserving machine learning and allows information verification (e.g., age verification) without requiring sensitive data disclosure. Data obfuscation tools can leak information if not implemented carefully however. Anonymised data for instance can be re-identified with the help of data analytics and complementary data sets.
- **Encrypted data processing tools** include homomorphic encryption, multi-party computation including private set intersection, as well as trusted execution environments. Encrypted data processing PETs allow data to remain encrypted while in use (in-use encryption) and thus avoiding the need to decrypt the data before processing. For example, encrypted data processing tools were widely deployed in Covid tracing applications. These tools have limitations however. For instance, their computation costs tend to be high although tools are emerging that address this limitation.

- **Federated and distributed analytics** allows executing analytical tasks upon data that are not visible or accessible to those executing the tasks. In federated learning, fo example, a technique gaining increased attention, data are pre-processed at the data source. In this way, only the summary statistics/results are transferred to those executing the tasks. Federated learning models are deployed at scale, for instance, in predictive text applications on mobile operating systems to avoid sending sensitive keystroke data back to the data controller. Federated and distributed analytics requires reliable connectivity to operate however.
- **Data accountability tools** include accountable systems, threshold secret sharing, and personal data stores. These tools do not primarily aim to protect the confidentiality of personal data at a technical level and are therefore often not considered as PETs in the strict sense. However, these tools seek to enhance privacy and data protection by enabling data subjects' control over their own data, and to set and enforce rules for when data can be accessed. Most tools are in their early stages of development, have narrow sets of use cases and lack stand-alone applications.

The high potential of PETs to protect the confidentiality of (personal and non-personal) data is recognised, and with this its potential to help raise the level of privacy and data protection and promote the rights of individuals. However, apart from a still limited number of solid and convincing data processing use cases, there is also agreement that the level of maturity of PETs is still unequal.

The role of PETs for implementing the OECD Privacy Guidelines' Basic Principles

PETs offer new functionalities that can assist with the implementation of the basic privacy principles of the OECD Privacy Guidelines on collection limitation, use limitation and security safeguards. To some extent, PETs can also support the individual participation and accountability principles.

However, PETs can also challenge the implementation of certain basic privacy principles. For example, data controllers using encrypted data processing tools may lose the ability to "see" data feeding into their models. This can contradict the need for personal data to be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, to be accurate, complete and kept updated ("data quality principle").

PET should not be regarded as "silver bullet" solutions. They cannot substitute legal frameworks but operate within them, so that their applications will need to be combined with legally binding and enforceable obligations to protect privacy and data protection rights.

Regulatory and policy approaches to PETs

PETs are often addressed explicitly and/or implicitly in countries' privacy and data protection laws and regulations through: legal requirements for privacy and data protection by design and by default; requirements for de-identification, digital security and accountability; and/or regulatory mandates to PEAs to further promote adoption of PETs.

These measures are often complemented by guidance issued by governments or PEAs that help clarify the measures. However, regulators tend not to adopt definitive positions on the merits of certain PETs to meet specific legal requirements, for example on cross-border data transfers, which underscores the difficulty in definitively validating specific PET solutions in a rapidly evolving landscape.

In addition, countries have adopted a wide variety of policy initiatives to promote innovation in and with PETs. They do this through research and technology development, adoption of secure data processing platforms, certification of trusted PETs, innovation contests, regulatory and other sandboxes and deployment of digital identity solutions.

1 Introduction

This section introduces privacy-enhancing technologies (PETs), setting out the main aims of the report for policy makers and regulators. It explores how paradigms for protection of confidentiality, integrity and availability of data (data security) are evolving. It further suggests that PETs can become the foundation of a new paradigm of privacy and data protection since they provide more control to data subjects and help enhance trust in the processing of data.

1.1. The emergence of privacy-enhancing technologies

The collection and processing of personal data have changed in ways that could enable a more privacy protective use of personal data at a technical level, moving society closer to the process and practice of privacy by design. A broad set of approaches is emerging based on new cryptographic techniques and structural changes to how data are processed. These approaches are introducing new privacy and digital security protections into data collection and processing.

While not fundamentally new,[1] these digital technologies and techniques provide novel and approaches to accountability and data protection while it is in use. They may also slightly alter the data, while allowing them to be processed for certain uses without disclosing the information they contain. These approaches are often grouped together under the term “privacy-enhancing technologies”, or PETs. However, that term understates the essential role these disruptive technologies and approaches may have in data governance more broadly.

PETs alter how organisations gather, access and process data, particularly personal data. PETs are promising because they expand access to data analytics while increasing digital security and privacy and data protections. For example, PETs support collaborative analysis over data that would otherwise be too sensitive to disclose, combine and use across individuals or entities.

Governments and regulators, most notably privacy enforcement authorities (PEAs), have identified and emphasised these types of technologies as prominent solutions for privacy and personal data protection (EDPB, 2020[1]; ENISA, 2021[2]; OCP, 12 April 2021[3]; White House [United States], 2022[4]; ICO, 2022[5]). The 2022 Communiqué "Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces" from the Roundtable of G7 Data Protection and Privacy Authorities (G7, 2022[6]) recognises that

> *[t]he use of PETs can facilitate safe, lawful and economically valuable data sharing that may otherwise not be possible, unlocking significant benefits to innovators, governments and the wider public. In recognition of these benefits … the G7 data protection and privacy authorities … will seek to promote the responsible and innovative use of PETs to facilitate data sharing, supported by appropriate technical and organizational measures. (G7, 2022[6])*

The review of the implementation of the OECD (2013[7]) *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Privacy Guidelines), highlighted the need to examine PETs and their application to transborder data flows:

> *Responding countries also agreed that further guidance is needed on available technical and organisational safeguards. Specifically, responding countries and experts pointed to the need for an in-depth examination of opportunities and barriers in the use of emerging new privacy enhancing technologies (PETs), including their application to transborder data flows. (OECD, 2021[8])*

While some of these technologies are not new, many are evolving and may ultimately warrant a re-evaluation of regulations on data collection and processing. As one key challenge, these technologies often fall outside the radar of policy makers and regulators given their highly innovative nature of the technologies themselves and their application areas. In addition, the technologies are highly technical, creating a significant "language barrier" between engineers building these systems and the policy makers and regulators who will ultimately determine how to use them. These technologies, which are at different stages of development, will likely need to be part of broader data governance frameworks. This should ensure they are used in line with associated risks, including privacy risks, and that data are secure. Governments and PEAs will increasingly need to consider how personal data are collected and processed with PETs and how these technologies fit into their privacy and data protection frameworks.

1.2. Goals of the report

This report is meant to introduce PETs and provide an assessment of their maturity in the current state of the art. As such, it is a high-level overview of key technological developments and their mechanisms rather than an in-depth and comprehensive survey and technical analysis. It will also provide policy makers and regulators, most notably PEAs, with background to help them better understand potential benefits, drawbacks and trade-offs associated with each type of technology. This assessment is based on the principles of the OECD Privacy Guidelines, and how specific PETs can help implement its principles.

The three goals of this report are to:

1. provide a non-technical introduction to PETs to policy makers and regulators in charge of data governance, privacy and data protection based on a taxonomy that reflects the impact of PETs' privacy and data protection mechanisms to facilitate the consideration of policy makers and regulators;

2. take stock of technological, policy and regulatory developments related to PETs and consider the opportunities and challenges of the different types of PETs in the context of the OECD Privacy Guidelines;
3. assist policy makers and regulators, most notably PEAs, to better consider the most recent technological developments on PETs for privacy and data protection, and data governance more broadly.

1.3. Evolving paradigms

The evolution of paradigms for protection of confidentiality, integrity and availability of data (data security) offers a good way to contextualise the changing landscape of privacy and data protection in respect to the new approaches to PETs. Data security is undergoing a significant evolution. Initially, security sought to protect data at the perimeter of the organisation. It is now moving to a new "zero trust" paradigm where the bad actors are already assumed to be inside the organisation. Digital security, then, is accomplished by locking down all data except for specific approved uses by authorised people. Zero-trust approaches in digital security have helped mitigate the risk of damage that a bad actor can cause if they can gain access to internal digital resources.

A similar evolution could be seen as emerging in privacy and data protection. Today, privacy and data protection still primarily rely on rules for how data can be collected, processed and used. Once the data are collected and/or transferred, "individuals then lose their capabilities to control how their data are re-used and to object to or (technically) oppose such uses and can rely solely on law enforcement and redress. The risks of loss of control are multiplied where the data are further shared downstream across multiple tiers, in particular when these tiers are located across multiple jurisdictions" (OECD, 2019[9]). This increases the risk for large-scale data breaches and misuse such as in the case of Cambridge Analytica (Isaak and Hanna, 2018[10]).

The evolving data governance paradigm enabled by PETs follows a similar trajectory to the zero-trust approach in digital security: trust is no longer assumed and personal data must remain protected in an adversarial environment. In this sense, PETs help ensure the continuity of privacy and data protection through technical means, even after data have been collected and eventually transferred to other entities, possibly including where these entities may be located out of the original jurisdiction. In so doing, they can effectively complement protection offered mainly by legal or contractual measures for such transfers. Therefore, PETs should not be regarded as a "silver bullet" solution to all privacy and data protection challenges. PETs, for example, do not necessarily help address issues related undue biases which may be reflected in the original data. Their use can also not guarantee the security of the entire information technology (IT) systems that rely on the data for which PETs are used.

1.4. Moving towards privacy and data protection by design

PETs can be seen as the underpinnings of a new paradigm of privacy and data protection that is evolving as described above. They provide more control to data subjects and enhance trust in the processing of data (compare with section above on zero trust). OECD research has long championed "privacy by design" (OECD, 2010[11]; OECD, 2013[12]), and PETs increasingly play a significant role in moving society towards these goals. Many of the technologies listed above have important implications for the related goal of "security by design" (OECD, 2012[13]). PEAs in countries such as Ireland, the United Kingdom and Republic of Korea, as well as the European Data Protection Board, have dubbed this new paradigm "data protection by design" [see Art. 25 of the European Union (2016[14]) General Data Protection Regulation (GDPR)]. The Royal Society (2019[15]; 2023[16]) highlights how advances in PETs can expand the possibilities for both privacy and utility. Instead of a traditional trade-off between privacy and utility, research and development in PETs can lead to increases in both utility and privacy protections.

In so doing, PETs can enable new applications and use cases. At the 2022 Asia Tech x Singapore (ATxSG 2022) roundtable on "Trust in Data", participants highlighted use cases linked to a higher outcome or a social good as examples where the value PETs could be perceived more easily (IMDA, 2022[17]). These include:

> *Managing pandemics by using PETs for building models which can predict metrics such as rate of infection, rate of hospitalization, etc;*
>
> *Facilitating ESG [environmental, social, and governance] reporting which often requires commercially sensitive data that could be kept confidential by use of PETs; and*
>
> *Prevention of financial crimes by using PETs for cross-border data flow.*

2 Current definitions and categorisations of PETs

This section begins with existing definitions and categorisations for PETs. These draw on diverse sources – from Canada, the United States and the United Kingdom to the European Union Agency for Cybersecurity and the OECD itself. It then proposes a new taxonomy for classifying PETs that incorporates data accountability, data obfuscation and encrypted data processing tools to address specific Basic Principles of the OECD Privacy Guidelines.

2.1. Towards a common understanding of privacy-enhancing technologies

Although the concept of privacy-enhancing technologies (PETs) is far from new and their use is spreading, it has never had a universally accepted definition. Over the years, different organisations have come up with definitions of PETs and the categorisations of the corresponding technologies. Each one has its own merits and deserves consideration. However, these definitions and categorisations were also influenced by the context in which they were developed. They reflect the state of technology at any given time or the purpose of a study or project that the PETs came to support.

The absence of a stable definition in this field can hinder a concerted analysis by policy makers, and privacy enforcement authorities (PEAs) in particular, of the potential impacts of PETs on data protection and privacy assessments.

Building on definitions and categorisation of PETs, this section proposes a new taxonomy for classifying PETs. It assigns each PET (whether old, emerging or eventual) to a category of technologies that addresses specific Basic Principle(s) of the OECD Privacy Guidelines. These categories are (i) data obfuscation, (ii) encrypted data processing, (iii) federated and distributed analytics, and (iv) data accountability tools. This taxonomy, which aims to be technology-neutral and robust over time, is based on the analysis of the privacy-preserving mechanisms of 14 PETs discussed in Section 3.

2.2. Existing definitions and their evolution

Before proposing a new categorisation that meets the main objective of this report, it seems useful to recall here the existing definitions and categorisations, as so many external references that can help to understand the evolution over time of the consideration of PETs in different communities.

The OECD (2002[18]) report on "Inventory of Privacy-Enhancing Technologies" provides a broad definition of PETs. It states:

> *Privacy-enhancing technologies (PETs) commonly refer to a wide range of technologies that help protect personal privacy. Ranging from tools that provide anonymity to those that allow a user to choose if, when and under what circumstances personal information is disclosed, the use of privacy-enhancing technologies helps users make informed choices about privacy protection.*
>
> *PETs can empower users and consumers seeking to control the disclosure, use and distribution of personal information on line. PETs can also aid businesses and organisations in enforcing their own privacy policies and practices. In an era of consumer concerns about online privacy, PETs are crucial tools in managing the flow of personal information on global public networks.*

According to Seničar, Jerman-Blažič and Klobučar (2003[19]), PETs are

> *(a) new breed of technologies … to help individual users control the amount of personal information they disclose in an on-line transaction. These technologies promise to enable individuals to take control over how their data is being collected. … The ultimate goal of these initiatives is to make informational self-determination a practical reality and to implement emerging policy frameworks—legislation and self-regulation—aimed at minimising the occasions in which violations of privacy are attempted by restricting certain practices.*

The European Union Agency for Cybersecurity (ENISA) refers to PETs 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 to privacy of an individual or a group of natural persons" (ENISA, 2016[20]). It further specifies that PETs "encompass … all kinds of technologies [according to above definition] that support privacy or data protection features (e.g. technologies that make use of privacy design strategies or consider protection goals for privacy engineering)." It also suggests that PETs are not restricted to data minimisation tools.

A report from the Office of the Privacy Commissioner of Canada (OPC) provides a review of tools and techniques for PETs. (OPC, 2017[21]) The report acknowledges that "many traditional security technologies (e.g. encryption) can be considered privacy-protective." Its study on PETs was

> *limited in scope to those technologies that protect information in transit (i.e. communicated/transmitted by information and communication technologies (ICT)). Technologies that protect information at rest (e.g., when stored on mobile devices) are not included, nor are descriptions of the ICT systems to which PETs may be applied (unless required for a proper understanding of PET functionality.*

In its invitation to participate in its privacy enhancing technology sandbox (IMDA, 2022[22]), Singapore's InfoComm Media Development Authority (IMDA) introduced PETs as technologies that

> *are based on cryptography, give data providers the ability to either disclose data for analysis but not in its original form (in techniques like Differential Privacy or Homomorphic Encryption), or allow insights to be pulled from data which remains undisclosed at all times (in techniques like Federated Learning or Multiparty Computing).*

According to the White House [United States] (2022[4]), "(p)rivacy-enhancing technologies (PETs) refer to a broad set of technologies that protect privacy" that include

> *privacy-preserving data sharing and analytics technologies, which describes the set of techniques and approaches that enable data sharing and analysis among participating parties while maintaining disassociability and confidentiality. Such technologies include, but are not limited to, secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic data generation tools.*

According to the Information Commissioner's Office (ICO) of the United Kingdom (2022[5]) "PETs are technologies that embody fundamental data protection principles by minimising personal data use, maximising data security and/or empowering individuals." Referring to the definition of ENISA (2016[20]), the ICO acknowledges that "the concept covers many different technologies and techniques."

The evolution of these definitions between the beginning of the 2000s and today reveals the paradigm shift that has taken place over the years. In particular, the fundamental challenge of privacy regulation through the 'notice & consent' approach in some jurisdictions has led to shift the burden of protection from the data subject (through the exercise of its right to informational self-determination) towards the organisation that processes the data and becomes accountable in this regard.

2.3. Existing categorisations

Given the wide variety of PETs, there is a need to categorise the various types of technologies to simplify governance and regulatory approaches and assessments. Several papers have put together lists of categories of PETs (Seničar, Jerman-Blažič and Klobučar, 2003[19]; Kenny, 2008[23]; OPC, 2017[21]; WEF, 2019[24]; OCP, 12 April 2021[3]; Asrow and Samonas, 2021[25]). The lists and groupings vary across these papers over time as new technologies emerge and mature.

It is useful to recall the different categorizations developed over the years, in particular to allow policymakers to identify whether some of them have been used as a reference for their own purposes. In the same way that the evolution of the various definitions above is indicative of the evolution of regulatory approaches to privacy, the categorisation of PETs is also indicative of their growing sophistication and the fact that they aim to respond to new issues, in a context where data has become ubiquitous.

The OECD (2002[18]) report categorises PETs into four broad categories based on where the technologies reside: personal, web-based, information brokers and network-based. This inventory includes technologies that were common or developing at the turn of the century. However, the technological changes over the past 20 years require an updated structure to describe today's evolving PET landscape. One of the biggest changes over the past two decades are significant advances in encrypted data processing. At the turn of the millennium, this technology was in its infancy.

ENISA published an assessment framework in 2016 that classifies PETs into categories by tool type (Montjoye et al., 2015[26]; ENISA, 2016[27]). These include secure messaging tools, virtual private networks, anonymising networks and anti-tracking tools. The categorisations are largely based on the prevailing technologies at the time. The treatment of encryption is largely focused on communication (in transit and at rest) instead of the new developments in encrypting data while in use.

OPC (2017[21]) presents a taxonomy of PETs based on the "functionality/capabilities that they provide to an end user", which include: (i) informed consent, (ii) data minimization, (iii) data tracking, (iv) anonymity, (v) control, (vi) negotiate terms and conditions, (vii) technical enforcement, (viii) remote audit of enforcement, and (ix) use of legal rights. The report highlights the difficulty of categorising technologies by functionality because certain technologies can offer different types of functionalities.

The US Federal Reserve Bank (FRB) of San Francisco published a report on PETs in 2021 that categorises technologies by their function (Asrow and Samonas, 2021[25]). Each category include specific technologies: Altering data (including anymisation, pseudonymisation, differential privacy and synthetic data); shielding data (encryption, homomorphic encryption, and privacy enhanced hardware); and systems + architecture (multi-party computation, data dispersion, management interfaces, and digital identity). The FRB categorisation represents the modern approach to categorising PETs based on their approach to privacy protection. For example, the first category focuses on tools that alter data such as anonymisation and differential privacy. In contrast, the second category contains tools that shield the original data. The "systems and architecture" category is challenging because it includes tools such as multi-party computation, which are encryption technologies in a system that shields data.

Although it does not focus on PETs, the National Institute of Standards and Technology (NIST) privacy framework can also be used to categorise PETs. It "provides a common language for understanding, managing, and communicating privacy risk with internal and external stakeholders" (NIST, 2020[28]). The NIST framework classifies privacy controls into five functional areas (identify, govern, control, communicate, protect) and lists 18 distinct categories within those functions. As one of its benefits, NIST is tightly integrated with its complementary security controls. The NIST categorisation is more focused on individual controls than classes of technologies.

2.4. Proposed working definition and taxonomy

For this report, PETs are understood as a collection of digital technologies, approaches and tools that permit data processing and analysis while protecting the confidentiality, and in some cases also the integrity and availability, of the data and thus the privacy of the data subjects and commercial interests of data controllers.

PETs typically are not stand-alone tools. Rather, they can be used in concert with other organisational and legal tools to implement data governance objectives. PETs may rely on each other to function. In the same way that chefs use a variety of ingredients to form a recipe for a dish, PETs are the ingredients that can be combined to achieve certain privacy and data protection objectives.

The next section presents the proposed taxonomy of PETs based on the following four categories: (i) data obfuscation, (ii) encrypted data processing tools, (iii) federated and distributed analytics, and data (iv) accountability. This taxonomy, which aims to be technology-neutral and robust over time, is based on the privacy-preserving mechanisms of 14 PETs discussed in more detail in Section 3.

3 Major types of PETs, their maturity, opportunities and challenges

This section analyses 14 different types of PETs which are classified in four broad categories. **Data obfuscation** tools embrace anonymisation/pseudonymisation, synthetic data and zero-knowledge proofs, among others. For their part, **encrypted data processing** tools comprise homomorphic encryption, multi-party computation, private set intersection and trusted execution environments. **Federated and distributed analytics**, including federated and distributed learning, allow executing analytical tasks upon data that are not accessible to those executing the tasks. **Data accountability** tools encompasses key technologies such as accountable systems and personal data stores. The section analyses the maturity of these PETs, including current and potential applications for setting and enforcing privacy rules, as well as related challenges and limitations.

3.1 Categories of privacy-enhancing technologies (PETs)

This section identifies 14 PETs based on research and development in the private sector, including academic institutions such as the Massachusetts Institute of Technology (MIT). Each one is described briefly below. The PETs are divided into the following four broad categories: (i) data obfuscation, (ii) encrypted data processing, (iii) federated and distributed analytics, and (iv) data accountability tools. Some of the 14 PETs can fit in more than one category; in which case they are assigned to a main category. It should also be noted that most PETs as discussed in this report do not address the risk of group harm that would result from potential misuse of insights gained from analysing data that are made available through PETs.2 Table 1 gives the overview of the four major types of PETs and their opportunities and challenges.

Table 1. Overview of major types of PETs, their opportunities and challenges

Types of PETs	Key technologies	Current and potential applications*	Challenges and limitations
Data obfuscation tools	Anonymisation / Pseudonymisation	Secure storage	- Ensuring that information does not leak (risk of re-identification) - Amplified bias in particular for synthetic data - Insufficient skills and competences
	Synthetic data	Privacy-preserving machine learning	
	Differential privacy	Expanding research opportunities	
	Zero-knowledge proofs	Verifying information without requiring disclosure (e.g. age verification)	- Applications are still in their early stages
Encrypted data processing tools	Homomorphic encryption	Computing on encrypted data within the same organisation Computing on private data that is too sensitive to disclose Contact tracing / discovery	- Data cleaning challenges - Ensuring that information does not leak - Higher computation costs
	Multi-party computation (including orivate set intersection)		
	Trusted execution environments	Computing using models that need to remain private	- Higher computation costs - Digital security challenges
Federated and distributed analytics	Federated learning	Privacy-preserving machine learning	- Reliable connectivity needed - Information on data models need to be made available to data processor
	Distributed analytics		
Data accountability tools	Accountable systems	Setting and enforcing rules regarding when data can be accessed Immutable tracking of data access by data controllers	- Narrow use cases and lack stand-alone applications - Configuration complexity - Privacy and data protection compliance risks where distributed ledger technologies are used - Digital security challenges - Not considered as PETs in the strict sense
	Threshold secret sharing		
	Personal data stores / Personal Information Management Systems	Providing data subjects control over their own data	

Note: (*) Only one application has been included for the sake of readability.

3.2. Data obfuscation tools

3.2.1. Key technologies and their maturity

Data obfuscation tools, as the name suggests, obfuscates data by processing the data locally, including on the data subject's device, altering the data by adding "noise" or by removing identifying details. These tools like many of the other tools discussed in the following section rely on cryptography as a key enabler (see Box 1).

Box 1. Cryptography as a key enabler for privacy-enhancing technologies

Many studies (e.g. OECD, 2002[17]; ENISA, 2016[19]; OPC, 2017[20]) have recognised encryption as a "traditional security" and "privacy-protective" technology that can obfuscate data in transit (i.e. transmitted through digital technologies), at rest (e.g. stored on a storage device), and at use (i.e. encrypted data processing, see Section 3.3).

Cryptography is a key enabler for many of the tools presented in this section. An example includes the use of cryptographic tools to enable pseudonymisation. These include e.g. (i) (one-way and collision free) cryptographic hash functions that are used to map input strings to generated pseudonyms as well as (ii) the use of block cipher like the Advanced Encryption Standard (AES) to encrypt an identifier (using a secret key, which is both the pseudonymisation secret and the recovery secret). (ENISA, 2019[29]; ENISA, 2021[2]) Other more recent and advanced examples discussed in this report include zero-knowledge proof (ZKP), homomorphic encryption (HE) and (secure) multi-party computation (MPC).

Examples of data obfuscation tools include:

- **Anonymisation**: Anonymisation is the process of removing identifying elements from data to prevent re-identification of the data subject. Anonymised data, therefore, should in theory not be linkable back to an individual even when combined with additional data sets.

  Anonymisation has been used widely as it promises to remove identifying details from data so they can be used in a way that does not violate the privacy of data subjects. In practice, anonymisation has been used as clear lines that either allow or disallow data usage in certain situations. However, true anonymisation with explanatory power is difficult to achieve and remains elusive. Researchers continue to re-identify "anonymised" data by matching with other available data sets.

  As anonymisation is widely deployed it is also widely referenced in national (and sub-national) legislation as an acceptable method for rendering personal data so their use falls out of the scope of privacy and data protection frameworks. This is because anonymised data by definition can no longer be considered personal data.[3] "Once data is truly anonymous and individuals are no longer identifiable, the data will not fall within the scope of the GDPR" (EDPS, 2021[30]). However, these legislative frameworks may vary significantly in their requirements for what counts as anonymised as they may use different standards for the acceptable degree of identifiability.

- **Pseudonymisation**: Compared to anonymisation, pseudonymisation is a weaker form of de-identification. It involves removing potentially identifiable information from the data to reduce the risk of identification of the data subject, although some residual risk remains. Pseudonymised data preserves their potential to be reconstructed when combined with remotely stored, identifiable information or with outside identifiable data sets.

  Pseudonymisation is also widely used as it can remove identifying details from data, but in a much more easily reversible manner compared to anonymisation. In contrast to anonymised data, however, pseudonymised data are considered personal data in many jurisdictions (see section 4.1.3).

- **Synthetic data**: Synthetic data is "[a]n approach to confidentiality where instead of disseminating real data, synthetic data that have been generated from one or more population models are released." (OECD, 2005[31]) One can distinguish between fully synthetic[4], partially synthetic[5] or hybrid[6] data. (Léautier, 2022[32]) The main idea is to generate artificial data with similar statistical properties to an original data source.

"The challenge is to have data that are still useful for the set purposes, e.g. medical research, because they maintain the same statistical properties as the original data, but are no longer those originally collected from individuals." (European Data Protection Supervisor, 2021[33]) There is consensus that the use of synthetic data can reduce the privacy risks. However, challenges remain. According to the Office of the Privacy Commissioner of Canada (OPC, 2022[34]), for instance "[r]e-identification is still possible if records in the source data appear in the synthetic data". Furthermore, similar to anonymisation and pseudonymisation, synthetic data are also susceptible to re-identification attacks (Stadler, Oprisanu and Troncoso, 2020[35]), and they also do not protect against attribute disclosure.[7]

- **Differential privacy**: These techniques make small changes (add noise) to the raw data to mask the details of individual inputs, while maintaining the explanatory power of the data. The idea is that small changes to individual records can securely de-identify the inputs without having a significant impact on the aggregated results. Noise can be added at the time of data collection (distributed) or at the central location before the data are released (centralised) (Royal Society, 2019[15]).[8]

  Differential privacy is relevant as a PET because it provides data subjects with some protection of deniability in cases where someone attempts to re-identify released data. Noise introduced into the dataset should not alter any large-scale analysis but makes any individual data less reliable and protective for the data subjects. Policy makers may need to provide guidance about the amount of noise that must be introduced to protect the privacy of data subjects.

  Differential privacy is well developed in academia but only deployed at scale by few organisations. (Drechsler, 2021[36]) More development is needed to define acceptable parameters and thresholds for differential privacy in different use cases (Apple, 2017[37]). Many of the deployments of differential privacy discussed in the literature have been criticised for choosing parameters that either do not provide enough privacy protection or enough utility.[9]

- **Zero-knowledge proofs (ZKP)**: There are times when it is useful to prove that something is true or false without disclosing any additional information in the query. ZKP can answer the simple question of whether something is true or false without revealing any additional information. They hide the underlying data while answering simple questions such as whether someone's income is above a certain threshold.

  ZKP can enhance privacy and data protection where they can eliminate the need for data subjects to turn over personal data for routine uses such as verifying sensitive information as part of any application process, e.g. verifying if prospective renters have an income over a predetermined threshold or individuals have a minimal age (Box 2). ZKP could thus help shift the paradigm from requiring users to reveal their sensitive information as part of a transaction to instead allow others to verify the claims.

  ZKP offer important properties for preserving privacy, but applications are still in their early stages. They have focused primarily on improving the privacy of cryptocurrency applications. There is discussion about using ZKP in health, for elections, age verification and traffic management in the future but no large-scale deployments to date. This could change though as ZKP are increasingly considered for the implementation of digital identity management systems. ZKP is for example recognised as one of the key technologies underpinning the future European digital identity wallets that are being planned as part of the proposed European Union (2021[38]) regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). See Section 3.4 on data accountability tools and personal data stores / personal information management systems in particular.

Box 2. ZKP enabled privacy-preserving age verification: Implementation of a demonstrator

The innovation lab of the French data protection authority (Laboratoire d'Innovation Numérique de la CNIL, LINC) presented a demonstrator of an "ideal" digital solution for age-verification that relies on ZKP. This demonstrator was used to prove that an age verification system is feasable, through a third-party system, that protects the identity of individuals as well as guarantees the principle of data minimization.

The demonstrator is based on the following three entities that are highlighted as necessary for the setup of the ZKP enabled age-verification system, i.e. :

- A website requiring age-verification for access to its content (service provider)
- One or more "certified" websites to verify the user's real age (certified third party)
- A "trusted" authority granting certification of those third parties (certifying authority)

For the age-verification procedure, the proof-of-age to be used by the service provider includes neither the user's real identity nor the identity of the certified third party that provides the proof-of-age. Furthermore, the certified third party has no information whatsoever on the purpose of this verification, and the user's information including browsing habits remains confidential. This requires however that the certifying authority provides the technical specifications (e.g. protocol and data format) for implementing the age verification system as well as a list of revoked keys of certified third parties.

The LINC provides the source code of the demonstrator via Github[1], Adullact[2] and dockerhub.io. The source code is freely modifiable and reusable, commercially or not, under reserve of being credited.

Note: 1. https://github.com/LINCnil/SigGroup (accessed on 1 February 2023)
2. https://gitlab.adullact.net/linc/siggroup (accessed on 1 February 2023)
Source: (Gorin, Biéri and Brocas, 2022[39])

3.2.2. Current and potential applications

- **Verifying information without requiring disclosure**: Data subjects often are required to reveal personal data about themselves such as their age or income information to obtain services. Obfuscation PETs such as ZKP can confirm information without revealing it and could have applications in health care, government, housing and e-commerce (see Box 2 on age verification).
- **Expanding research opportunities**: Obfuscation PETs such as differential privacy can support new research opportunities for large data sets that were otherwise too sensitive to share. It becomes much more difficult to confirm if data on an individual are true or include noise. Prime applications include sectors with large amounts of sensitive, valuable information such as health care, transportation and finance.
- **Secure storage**: Obfuscation techniques such as differential privacy can reduce the risk that erroneously exfiltrated data can be positively identified and confirmed. Pseudonymising data with identifying details securely stored in a separate location can reduce risk of re-identification if the data are exfiltrated.
- **Re-use and sharing of data where only the overall statistical properties need to be preserved**: By preserving the overall statistical properties, analysing synthetic data can lead to the same statistical conclusions as the analysis of the original data source. Prominent application areas include, but are not limited to, (i) training AI models (Hawkins, 2021[40]; Sacolick, 2022[41]), (ii) testing software (Sacolick, 2022[41]; GenRocket, n.d.[42]), (iii) sharing data including for the purpose

of official statistics (United Nations Economic Commission for Europe, 2022[43]), and (iv) the generation of synthetic digital content[10]. (Léautier, 2022[32])

3.2.3. Challenges and limitations

- **Anonymisation techniques are not fully reliable**: Records from anonymised data sets are commonly re-identified after their release. This highlights the challenge of removing personal elements while still maintaining the explanatory power of the data (Narayanan and Felten, 2014[44]; Henriksen-Bulmer and Jeary, 2016[45]; Rocher, Hendrickx and de Montjoye, 2019[46]). This challenge is to a large extent due to the difficulty of anticipating all means of re-identification at the time of the anonymisation: e.g. every possible set of data that could later on be combined with the anonymized dataset to reveal personal information as well as future technologies and analytical techniques that might arise to help re-identify individuals.
- **Other obfuscation measures can also leak information unintentionally**: Applications such as differential privacy introduce noise to records, but some records may be left in their original state. Data subjects gain the benefit of deniability about the veracity of a record, but the amount of data leakage is related to how much noise was introduced. For now, there are no agreed-upon norms for how much noise is required to protect privacy in different scenarios. Further, it is unclear whether a good privacy-utility trade-off exists for many real-world datasets given that parameter values that are sufficient to protect privacy may obliterate utility or vice versa. For example, large-scale implementations of differential privacy by some businesses have been considered to have insufficient privacy protection. (Tang et al., 2017[47])
- **Insufficient skills and competences**: Obfuscation measures including anonymisation often involves complex processes that would need to be implemented by trained data scientists to ensure that no information is leaked unintentionally. However, not all organisations will have the capacity and resources needed to implement such complex processes, and in some instance not even the awareness and the needed competences (know-how) about data analysis to realise and address the risk of re-identification.
- **Lack of current use cases**: Obfuscation PETs are promising, but there are relatively few current use cases. Some technologies such as ZKP have found niche uses in cryptocurrency applications, but there is significant room for growth.

3.3. Encrypted data processing tools

3.3.1. Key technologies and their maturity

Encrypted data processing tools represent the most important step forward in private data processing among the PETs presented in this report. Data processing has always been a major point of vulnerability from both digital security and privacy protection perspectives. This is because data needed to be available in the clear to be processed. With data at rest and in transit, common encryption techniques partly alleviate the risk of breaches. However, these risks still exist when data need to be decrypted at the time of processing.

Recent technological developments are changing the paradigm so that data can remain encrypted while in use. Encrypted data processing tools allow computations to run over data that are never visible or disclosed. In contrast to data obfuscation, the underlying data remains unmodified but hidden by encryption. The techniques have been known for a long time, but only recently have computers been strong enough to deploy them. These PETs could have a profound effect on data privacy and likely warrant reconsideration of how encrypted data processing is considered under the law. That said, it is important to acknowledge that encrypted data processing tools do not guaranty protection against digital security breaches given that serious data leakage can still occur through other ways.[11]

Examples of encrypted data processing tools include:

- **Homomorphic encryption (HE)**: Standard data processing methods require data to be visible to the organisation processing the data to be used. HE computes over encrypted data that the organisation never can see. The data subjects locks the data (with a key only they have) before passing them on to the data processor. The processor can then perform simple (but increasingly complex) calculations over the encrypted data to extract an encrypted result that can only be unlocked with the data subject's key.

  HE can enhance privacy and data protection because it allows data to remain encrypted while in use. This allows data subjects or controllers to maintain strict confidentiality over their data in cases where previously it needed to be visible for use in analysis. It thus reduces the security risks of data in use. As HE applications appear, policy makers will need to assess how the processing of encrypted personal data used in these models should be treated under the law.

  Homomorphic computation methods are used in other PETs such as multi-party computation (MPC, see below) and are widely trusted and increasingly deployed. However, homomorphic computation on its own is much less efficient than standard data analytics. Consequently, it takes longer and costs more in computation power. This trade-off between efficiency and privacy means that homomorphic encryption is only optimal for cases where the privacy benefits can justify the increased costs of computation and analysis. For now, most applications are done at a small scale. However, that could change with a stronger policy push for encrypting data in use and as the process becomes more efficient.

- **Multi-party computation (MPC)**: MPC is a set of tools that enables the participating parties to jointly compute a function over their input data while keeping those input data private. Essentially, it removes the need for a trusted third party to view and manage the data. MPC can aggregate sensitive data without requiring any data contributor to disclose their own data. As a result, secret sharing techniques or HE can be used to aggregate and compute over data from multiple parties.

  MPC is a promising PET because it allows data to remain encrypted or hidden while in use and aggregated without the need for a trusted third party. Data subjects can be guaranteed their data will remain secure and private during data processing. MPC reduces the security risks of data while they are in use. As with HE, policy makers may need to consider how encrypted data used in MPC are treated under the law.

  MPC applications are slightly more mature than stand-alone HE applications. This is largely because researchers continue to identify opportunities for private data processing, and these are increasingly done at scale.

  Private set intersection (PSI) is a form of secure MPC that allows organisations to find common elements in their datasets without revealing the contents of their respective data sets. PSI reveals only the shared elements across the different datasets. It can be used to link individuals or data elements across organisations for a variety of use cases.

  PSI can enhance privacy and data protection. It can reduce the privacy threat surface by revealing only the common elements of two data sets without requiring both data subjects to reveal their full sets to the other. Policy makers could require that companies looking to match customer lists use PSI to limit unnecessary data exposure. Regulators have also considered using PSI themselves as part of their supervisory work, including in a cross-border environment. For example, financial market regulators have explored how to leverage PSI to look for systemic risk based on undeclared financial relationships. (Bruno et al., 2018[49]; FATF, 2021[50])

  PSI techniques have been used in large-scale applications such as COVID-19 contact tracing functionality provided by Apple and Google. In this application, the phone can notify users if they have been in close contact with the phone of someone else who contracted the virus. They are also used extensively by mobile messaging apps to do contact discovery – determining whether a user's contacts are also on the app. PSI represents one of the most advanced uses of both MPC and HE.

- **Trusted execution environments (TEE)**: A trusted execution environment (TEE) is a dedicated area on a computer processor that is separated and secured from the operating system. It holds sensitive, immutable data and can run secure code within its secure confine. TEE assumes the operating system is corruptible and untrustworthy. Consequently, under TEE, the operating system cannot access information in the secure area of the processor or read the stored secrets. TEEs provide a secure location where data can be stored and used without exposing them to the risks of an untrusted environment.

  TEEs can help enhance privacy and data protection where they allow data to remain protected during use on a device. They can provide a safe storage space on the device for data that need to remain private. As TEEs become more common, developers will have more opportunities to move sensitive data and analytics into the TEE portion of the processor. Regulators could push for more use of TEEs. Major chip manufactures such as ARM, Intel and Qualcomm and software providers such as Apple, Google and Samsung have implemented TEEs on their devices.

3.3.2. Current and potential applications

- **Computing on private data that is too sensitive to disclose**: HE and MPC both allow computation using data that are too sensitive to disclose to a third party. Recent applications include using MPC to produce cyber risk metrics on security defences, control failures and losses (de Castro et al., 2020[51]), performing confidential wage surveys (Lapets et al., 2019[52]), linking education and tax databases in Estonia (Bogdanov et al., 2016[53]) and setting up double auctions for the Danish beet market (Bogetoft et al., 2009[54]).
- **Computing on encrypted data within the same organisation**: Sensitive data within an organisation remains encrypted while at rest and in transit. All four PETs in this category allow data to be analysed and processed while remaining protected. Some protocols focus on MPC (see section below), but the same techniques can secure data processing on an organisation's own data sets. This improves security in the case of a data breach.
- **Computing using models that need to remain private**: Organisations often have proprietary models they do not want to reveal while data subjects/owners have data they do not want to disclose. MPC, HE and TEE can all allow the models running a computation to remain private.
- **Contact tracing and mutual contact discovery**: PSI techniques have been used in large-scale applications such as COVID-19 contact tracing functionality provided by Apple and Google. In these cases, software can notify users if they have been in close contact with the phone of someone else who contracted the virus (Rivest et al., 2020[55]). Mobile messaging apps have also used PSI to do contact discovery – determining whether a user's contacts are also on the app – without disclosing all the contacts of users (Demmler et al., 2018[56]). PSI represents one of the most advanced uses of both MPC and HE.
- **Measuring online advertising conversions**: Researchers have used PSI techniques to match online advertisement delivery with payments for goods (Ion et al., 2020[57]).

3.3.3. Challenges and limitations

- **Data cleaning challenges**: Data controllers and processors are unable to examine and clean the encrypted data that are used for MPC, HE and PSI. Analysts typically gather data from sources, spend considerable time cleaning them and then use the data in their models. This is not possible using these PETs because the analyst can never see the raw data. All errors need to be identified and the data cleaned by the data subject or data controller submitting the data into the computation. Pre-processing checks are vital at the data subject level before data are submitted or errors will result and the computations will not converge to a solution.

- **Ensuring results do not leak information**: Encrypted processing tools are designed to secure data that are processed, but there are no guarantees that results will not leak information. For example, a query/computation that produces results from a single observation will leak the contents of that observation.[12] Therefore, special care has to be taken when choosing the function that will be computed with MPC for instance, as the result might leak information about the input data, just in the same way as this could happen if the function is computed by a trusted third party (Pence, 2022[48]). Research is exploring how to test whether computations could leak information in the results before the computation completes and the results are released (Pence, 2022[48]). These tests will need to be designed into systems and applications.
- **Higher computation costs**: Computations over encrypted data have significantly higher computation costs than a standard database query or application of a model. Organisations avoid using these techniques if simpler, less-expensive data processing in the clear is available. Government recommendations or requirements to use encrypted data processing could increase their use. The processes are also becoming more efficient as research advances.

3.4. Federated and distributed analytics

3.4.1. Key technologies and their maturity

Federated and distributed analytics allows executing analytical tasks (e.g. training models) upon data that are not visible or accessible to those executing the tasks. In this way, only the summary statistics or results are transferred to those executing the tasks. This allows sensitive data to remain under the custody of a data source while it is analysed by third parties.

Examples include:

- **Federated learning**: Traditional data analytical techniques require data to be linked and processed as a single dataset. With new federated learning methods, raw data are pre-processed at the level of the data source (e.g. at the level of the data subject). Only the summary statistics and results are transferred to the data processor to be combined with similar data from others. Federated learning reduces the need for sensitive data to leave the data subject's device and be stored by data processors.

  Federated learning can enhance privacy and data protection where it reduces the need for data controllers and processors to view and hold sensitive data from data subjects. Pre-processing the data locally at the data subject level means that sensitive data can stay with the data subject. Only learnt parameters from a model are transferred back to the data controller to be used in refining models. Policy makers may decide that certain data must be pre-processed locally to protect the sensitive personal data of data subjects.

  Federated learning is widely deployed by companies such as Google for predictive text applications. However, there remain concerns that the features/parameters pulled from federated learning can still leak personal information in certain cases (Hard et al., 2018[58]), and there are increasingly attacks that aim to recover some of the training data in certain cases. (Jiang, Zhou and Grossklags, 2022[59])
- **Distributed analytics:** This is a related but different method for spreading the analytics over multiple nodes. With distributed analytics, the data resides in a central location with the data controller, but the model training is spread across different nodes. This allows sensitive data to

remain under the custody of a data source while it is analysed by third parties. The European Commission's EU Data Strategy lists decentralized data processing as a method to improve user control and data protection compliance. (Janssen et al., 2020[60]) And the health sector has also expanded use of distributed analytics solutions for secure and privacy-protective use of health data for both public- and private-sector research. These include the EU Health Data and Evidence Network project, the European Medicines Agency Darwin project and the global Observational and Health Data Sciences and Informatics project (OECD, 2022[61]) .

Distributed analytics enables software and statistical analysis programmes to 'travel' to where data are located, rather than data flowing to a central data repository for analysis. Similarly to federated learning, this approach does not permit data analysts and processors to directly access data. All data to be used need first to be coded to a common data model, such as the Observational Medical Outcomes Partnership model.

3.4.2. Current and potential applications

- **Privacy-preserving machine learning**: Federated learning allows researchers to train models on data that stay local on the data subject's device. This prevents unnecessary collection and storage by the data controller. Currently, federated learning models are used to train predictive text applications on a large scale.

3.4.3. Challenges and limitations

- **Federated and distributed analytics can still leak information**: Federated learning applications, for instance, can leak information in the parameters that are sent back to the data controller. Researchers have proposed using encrypted data processing techniques such as homomorphic encryption or multi-party computation (both discussed above) to address the issue however (Zhou et al., 2021[62]).
- **Reliance on stable connectivity**: The use of federated and distributed analytics relies on a stable connectivity. This can be challenging for applications which require the continuous availability of the analytic results.

3.5. Data accountability tools

3.5.1. Key technologies and their maturity

Data accountability tools offer new controls over how data can be gathered, used or provide transparency and immutability into transactions. These tools are traditionally not considered as PETs in the pure sense given that they do not primarily aim to protect the confidentiality of personal data at a technical level. Yet they are frequently associated with PETs because they aim at enhancing privacy by providing new ways to require and enforce regulations about how data are processed, or by providing organisations and individuals with more agency and control over their data. Some have been in development for years yet are barely ready for broad adoption (accountable systems and personal data stores).

Examples of data accountability tools include:

- **Accountable systems**: These are software systems that manage the use and sharing of data and track compliance. They control and track how data can be collected, how they are processed and when they can be used. A key goal of accountable system design is to grant data access with limitations that are attached to, and follow, the data.

Accountable systems promise the ability to limit use of personal data outside the originally accepted scope. They can enhance privacy and data protection thanks to their ability to enforce rules and track compliance regarding use of personal data. Data rules and regulations could be integrated into the system to ensure compliance. For policy makers, though, these systems are not ready for practical implementation. The systems have struggled to grow at scale and get buy-in from necessary stakeholders. Therefore, they remain in pilot stages. While they may hold promise, their current applications are limited.

Accountable tools can take advantage of distributed ledger technologies (DLTs) such as blockchains to ensure the immutability of recorded data (inability to alter the data retroactively after they have been recorded). These DLT-enabled systems distribute copies of a ledger across multiple entities to ensure that a retroactive change to one ledger will be detectable and rejected by the other ledger holders. When used for accountable systems, private DLTs offer secure, immutable record keeping for how data are accessed, transferred or processed. This is beneficial for governance and compliance.[13] The distributed nature of DLTs can also make them less susceptible to digital security incidents.

This does not imply that DLTs are PETs and in fact the use of DLTs, and blockchain in particular, can even pose risks and challenges to privacy and data protection. The *OECD* (2022[63]) *Recommendation on Blockchain and Other Distributed Ledger Technologies* acknowledges that "Blockchain carries certain limitations and risks, some of which are specific to Blockchain while others are relevant to digital technologies more broadly, for example risks relating to privacy and security, custody of access credentials, and cryptography vulnerabilities".[14]

- **Threshold secret sharing (TSS)** – also known as Multi-party Computation Threshold Signing (MPCts): This cryptographic tool requires a predetermined number of keys to unlock encrypted data. It is the digital equivalent to a secure box that is locked with multiple separate locks, whose keys are held by different people. A predetermined number of key holders must all agree to use their keys to unlock it.

  TSS can enhance privacy and data protection because it can impose thresholds that must be met before data are available and accessible to data controllers. These thresholds could be agreed upon and set by data subjects or set via regulation. However, to date, little to no guidance is offered about thresholds that are safe for specific use cases. For example, what are best practices for threshold setting in different scenarios?

  TSS services are available on cloud platforms for specific use cases. For now, they have narrow applications. TSS also performs slowly on large data sets due to the cryptographic overhead. Current applications have largely targeted smaller amounts of data. For example, one work-around is using TSS to secure strong passwords rather than to secure the data themselves (Koens, 19 January 2021[64]).

- **Personal data stores / Personal Information Management Systems**: Current data processing techniques require organisations to collect data on individuals and store them in a large dataset that can then be used to process the data. Personal data stores switch the paradigm. They give control of personal data storage to individuals who can choose where and how they want their data stored, accessed or processed.

  Personal data stores (PDS) can enhance privacy and data protection where they provide users with more control over their own personal data as means to implement their data portability rights and enhance informational self-determination. (OECD, 2021[65]) In theory, they give users control over where their data are stored and how they are allowed to be used. PDS deployment and adoption faces some significant challenges. First, some PDS deployments put more responsibility for securing the data on the data subject rather than on data controllers/data processors, which have more resources and experience protecting data. The regulatory landscape was built with historical data paradigms in mind, making it challenging to determine regulatory responsibility among stakeholders. Janssen et al. (2020[60]) provide a detailed analysis of regulatory challenges for PDS within the General Data Protection Regulation (GDPR) framework.

Personal data stores enable users to manage their data at a granular level, allowing them to provide access to data and then revoke it. However, development has been slow, and most are still in the pilot stage. Private-sector companies such as Inrupt have raised funding, but no platform has successfully scaled yet. There are also significant barriers to adoption as the largest data platforms are likely reluctant to give up the current paradigm of data governance.

This could change however with the adoption of digital identity management systems such as "digital identity wallets" that have been defined for instance as part of the proposed European Union (2021[38]) eIDAS Regulation. These wallets are expected to allow "users to choose when and with which private service provider to share various attributes, depending on the use case and the security needed for the respective transaction". (European Commission, 2021[38]) In so doing these wallets would enable selective disclosure, which is one way of achieving data minimisation. (Zundel et al., 2022[66])

3.5.2. Current and potential applications

- **Providing data subjects control over their own data**: A key benefit of "data accountability PETs" is the promised ability to give data subjects ultimate control over how their data are used in given circumstances. This ensures that data are only used for approved purposes and by those who are allowed. In one system design, for example, the data subject maintains control of all their personal photos on a server under their control. Any outside users of those photos such as a social media platform would need to get access to them from the data subject's server (personal data store) before displaying them to other users. This structure would provide data subjects with granular control over how and when their personal data are used. In another case, accountable systems would attach "policies" to data that would dictate when and how data could be used.
- **Setting and enforcing rules regarding when data can be accessed**: Accountable systems and TSS both assign and enforce rules regarding when data can be accessed. A regulatory authority may impose limitations on when data can be used. These could attach to the data via data policies that would be enforced by a future accountable system. A TSS system can also enforce data access rules by requiring a predetermined number of keys for data to be decrypted.
- **Immutable tracking of data access, transfer and processing**: One key potential benefit of DLTs is their ability to track any access to, and transfer and processing of personal data that is held by data controllers as part of a larger accountable system. If the record of these data related activities is immutable, it can deter unauthorised use and be used in an audit trail during any examinations of inappropriate access.

3.5.3. Challenges and limitations

- **Narrow use cases**: Accountability tools have only been used in narrow use cases, even as market participants in most industries look at whether tools such as blockchain can be deployed efficiently in their own context. For now, there is no blanket use case that policy makers would likely consider. Each deployment will likely require a separate analysis that looks at the context and techniques used to protect data.
- **Lack stand-alone applications**: Accountability tools are typically deployed as one element in a larger system. Thus, they must be evaluated as components but also in the broader context of how they function and interact within the larger system. A PET may be secure as an individual tool but could leak data if incorrectly implemented in a larger system.

- **Configuration complexity**: Accountability tools promise to give more-granular data control to data subjects, but that control comes with increased complexity. Researchers have shown that as complexity increases, a system's understandability decreases. This, in turn, can lead to unmanageability and unpredictability (Reeves et al., 2020[67]). Individual users may be overwhelmed with the configuration choices they face in future accountable systems. This may require improved user interfaces (UI) and user experience (UX) of data accountability tools, as well as new market intermediaries who can help manage system configuration for users (Acquisti et al., 2017[68]). The latter is a viable option, however, only as long as these intermediaries remain trustworthy and their control over personal data do not lead to a re-intermediation of personal data controllers. (OECD, 2021[65])
- **Digital security challenges**: Personal data stores, in particular, open new security challenges for protecting personal data. They move responsibility for defending the data from data controllers (who may have more resources and good security practices) to data subjects or third parties (who may lack the skills or scale to successfully protect personal data). (OECD, 2021[65])
- **Adoption DLT enabled accountability tools is limited and raises privacy related challenges**: DLTs are typically slower and less efficient than centralised databases. That trade-off limits adoption to narrow use cases. The transparency of some DLTs can also introduce concerns related to the privacy of individuals involved, even where private blockchains are used. This raises potential privacy and data protection (compliance) challenges[15] and limits the scope of DLT that can be adopted for accountability tools or requires the combined used of other PETs[16] (Zyskind, Nathan and Sandy Pentland, 2015[69]; Frankle et al., 2018[70]).

4 Regulatory and policy approaches to PETs

This section takes stock of the regulatory and policy approaches to PETs across OECD members and partner economies. It examines issues such as providing guidance, legal requirements for data protection by design and by default, as well as requirements for de-identification, data security and accountability, and regulatory mandates. The section ends with an assessment of responses to a questionnaire that was circulated to OECD members and partner economies in 2022 (the PET Questionnaire) on how they are promoting innovation through research and development, secure data processing platforms, certification of trusted PETs, innovation contests, regulatory sandboxes, digital identity solutions and PETs for official statistics.

4.1. Legislation and guidance on the use of PETs

The results of the PETs questionnaire suggests that PETs are often addressed explicitly and/or implicitly in countries' privacy and data protection laws and regulations. This is typically done through (i) legal requirements for privacy and data protection by design and by default, (ii) de-identification requirements, (iii) digital security requirements, (iv) accountability requirements and/or (v) regulatory mandates.

To complement the above measures, governments or privacy enforcement authorities (PEAs) have issued guidance, which functions as supplemental material to help clarify rules.

4.1.1. Guidance on PETs

In 2017, the Office of the Privacy Commissioner (OPC) of Canada issued a report on "Privacy Enhancing Technologies – A Review of Tools and Techniques" with the objective to address the knowledge gaps on these tools and techniques (OPC, 2017[21]). The OPC has also published, in 2021, a blog post outlining how PETs can support the data privacy efforts of business. (OPC, 2021[71]) It focusses on "a few of the PETs that have emerged since that report", including: (i) federated learning; (ii) differential privacy; (iii) homomorphic encryption; and (iv) secure multiparty computation.

In 2019, the European Data Protection Board also provided guidance on PETs. It covers the role of controllers and clarifies, for instance, why and how controllers should have data protection designed into the processing of personal data and as a default setting throughout the processing lifecycle. If mature, PETs can be employed as a measure in accordance with Article 25 GDPR if the data controller uses an appropriate risk-based approach. PETs alone, however, are not automatically sufficient to cover the requirements in Article 25. However, controllers can assess whether a PET implementation would be an appropriate measure to achieve the objectives of the statute.[17]

After Türkiye's By-Law on Erasure, Destruction or Anonymization of Personal Data became effective in 2018 (see Section 4.1.3), Türkiye's Data Protection Board published its "Guidelines on the Deletion, Destruction or Anonymization of Personal Data" to clarify how data controllers should implement the procedures and principles in practice. In addition to its recommendations and best practices, the Guidelines also highlight the risks of re-identification (related to e.g. data linkage and the use of data analytics) that data controllers should address.[18]

The Information Commissioner's Office (ICO) of the United Kingdom released draft guidance on PETs for public consultation in September 2022, one of the most comprehensive examples to date of guidance for PEAs. The guidance examines PETs such as homomorphic encryption, secure multi-party computation, federated learning, trusted execution environments and zero-knowledge proofs (ZKP), and their application in a wide range of sectors. The ICO is also running a call for views on its updated draft guidance on "Anonymisation, Pseudonymisation and PETs" (ICO, 2022[72]). This looks at how PETs and anonymisation should be interpreted in regulation and the role of PETs in safe data sharing. These initiatives complement the initiative by the United Kingdom's Centre for Data Ethics and Innovation (CDEI), which has put together a comprehensive interactive guide to PETs (CDEI, n.d.[73]) and a repository of use cases on PETs (CDEI, n.d.[74]).

4.1.2. Legal requirements for data protection by design and by default

PETs can sometimes be directly linked to implementation of concrete provisions in national laws. The most emblematic recent example is the European Union (2016[14]) General Data Protection Regulation (GDPR), several articles of which refer to or are meant to cover the use of PETs. Respondents to the PET Questionnaire most frequently cite Article 25, which deals with "data protection by design and by default" (DPbDD). It specifies that data controllers

> *shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. (European Union, 2016[14])*

The United Kingdom has no specific legislation governing use of PETs. However, the United Kingdom's (2018[75]) Data Protection Act (the implementation of the GDPR) also includes a requirement for data protection by design and by default. It requires data controllers to implement appropriate technical and organisational measures, when processing personal data, to ensure compliance with data protection principles. PETs form part of the tools and methods data controllers can use to comply with data protection principles.

In certain jurisdictions, DPbDD has not been mandated by law or regulation but is rather based on best practices and guidance (see Section 4.1.1). Canada's federal *Privacy Act* (which applies to federal government institutions), for instance, does not contain provisions that applies to PETs specifically. But institutions do apply the principles related to privacy by design and building in privacy protections when implementing new or updating existing programmes, based on best practices albeit not on legal, regulatory or policy requirements.[19]

4.1.3. De-identification requirements

Organisations can use "de-identification" to comply with provisions under national data protection and privacy laws, or even to disallow application of these laws to the processing of specific data, in some circumstances. According to the *OECD* (2016[76]) *Recommendation on Health Data Governance* "[d]e-identification means a process by which a set of personal health data is altered, so that the resulting information cannot be readily associated with particular individuals. De-identified data are not anonymous data." Anonymization and pseudonymization therefore need to be distinguished from one another, since legal requirements under national laws vary between these processes.

Article 25 GDPR on DPbDD mentions pseudonymisation as a method for implementing appropriate technical and organisational measures to support the data protection principles. According to Article 4 (5):

> *"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*

In contrast, anonymous data is considered outside the scope of the GDPR. In Recital 26 GDPR, data are anonymous when "information which does not relate to an identified or identifiable natural person or to personal data (is) rendered anonymous in such a manner that the data subject is not or no longer identifiable." Opinion 05/2014 of the (former) "Article 29" working group provides guidance on anonymisation techniques. This opinion is being revised within the European Data Protection Board.

Article 3, Paragraph 7 of Korea's Personal Information Protection Act recommends that the personal information controller use pseudonymised data during collection of personal information if at all possible, even if the personal information is processed using a pseudonym. In April 2022, the government of Korea published Guidelines for Handling Pseudonymised Information that highlights tools that the personal information data controller can use for the general task of pseudonymisation. These include differential privacy and homomorphic encryption (HE), among others. The Korean government also issued guidance relative to development of artificial intelligence (AI) in its "AI Personal Information Protection Self-Checklist" in May 2021. The document recommends use of PETs to protect personal information and prevent privacy infringement in developing or operating AI technologies and services.

Both the Federal Data Law and the General Data Law of Mexico provide a definition of dissociation: "(t)he procedure by which personal data cannot be associated with the holder or allow, by its structure, content or degree of disaggregation, the identification of the holder."

Article 7 (1) of Türkiye's Personal Data Protection Law, No. 6698, on "erasure, destruction or anonymization of personal data" requires that "personal data shall be erased, destructed or anonymized by the data controller, ex officio or on the request of the data subject, in the event that the reasons for the processing no longer exist." The procedures and principles for the erasure, destruction or anonymization of personal data are laid down in Türkiye's By-Law on Erasure, Destruction or Anonymization of Personal Data as stipulated by Article 7 (3) of the Personal Data Protection Law. According to Article 10 (1) of the By-Law, "[a]nonymization is the process of rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data."[20] And according to Article 10 (3) "[t]he data controller is obliged to take any type of technical and organizational measures required for ensuring anonymization of personal data".

In the United States, the protection of health data is governed by the Health Insurance Portability and Accountability Act of (1996[77]) (HIPAA). The law includes a de-identification standard that determines whether data are considered personally identifiable. § 164.514 HIPAA states:

> *Other requirements relating to uses and disclosures of protected health information.*
> *(a) Standard: de-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. (United States Congress, 1996[77])*

The United States Department of Health and Human Services issued guidance regarding the re-identification standard in 2012. The guidance provides two methods that can be used for de-identification – expert determination and safe harbour. In the former, experts determine whether the data de-identification approach applied to data will result in only a very small risk that an anticipated recipient could re-identify an individual. Conversely, the safe harbour approach specifies 18 types of identifiers that must be removed. It states that no actual knowledge or residual information can be used to re-identify an individual.

It is worth noting that the California Consumer Privacy Act defines "de-identified information" as: "(d)ata, which cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer."

Canada's proposed Consumer Privacy Protection Act (CPPA), which was part of a bill tabled in Parliament in June 2022, provides a few incentives for PETs and addresses their potential use. For example, the bill proposes a definition of de-identify that clarifies how to treat personal information that has been made less identifiable but is not anonymous. The proposed legislation would, if passed, regulate how the law would apply to such information. The law also proposes a definition for "anonymise" and scopes anonymised information out of the application of the Act (House of Commons [Canada], 2022[78]).

> *Definition: **anonymize** means to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means.*
>
> *Definition: **de-identify** means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains.*

The United Kingdom's Data Protection and Digital Information Bill, introduced in Parliament in July 2022, creates a legal test for determining when data will be regarded as personal or anonymous while they are being processed. The measures aim to confirm that the test for whether anonymous data can be re-identified is relative to the means available to the controller to re-identify the data. Coupled with upcoming guidance from the Office of the Information Commissioner of Canada, this will provide organisations with clarity about the use of PETs to meet their compliance obligations. To that end, it will include information on organisational measures that may need to be put in place to ensure PETs meet legislative requirements on anonymisation. (See section 4.2 on Guidance by Privacy Enforcement Authorities on the use of PETs).

The Director-General of Israel's Ministry of Health issued its Circular regarding "Secondary Uses of Health Data" in 2018. (Ministry of Health [Israel], 2018[75]) The Circular broadly refers to anonymisation as a major and necessary principle in this field,[21] and stipulates the obligation of healthcare organisations exercising secondary uses with identified data to present a plan with a solution based on anonymisation, where anonymisation is possible (Article 5.5). The Circular also stipulates that Israel's Ministry of Health will determine acceptable minimal rules or technological measures for anonymisation, in order to have uniformity, which will facilitate cooperation between health organisations and other entities requiring a uniform and identical anonymisation mechanism.

4.1.4. Data security requirements

PETs commonly allow data controllers to implement data security obligations, especially in data protection laws.

Article 32 GDPR on "Security of personal data" states, for instance, that "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" (European Union, 2016[14]). The article then lists pseudonymisation and encryption of personal data as two appropriate measures. Data controllers are also instructed to ensure the ongoing confidentially, security and resilience of systems. Finally, data controllers need to be able to restore access to data in the case of an incident. They must also have a process in place to regularly test, assess and evaluate the effectiveness of implemented measures.

Mexico's Federal Data Law emphasises that all responsible parties that process personal data must establish and maintain physical and technical administrative security measures to protect personal data from damage, loss, alteration, destruction or unauthorised use, access or processing. Data controllers must not adopt security measures inferior to those they keep to manage their own information (Article 19). Mexico's PEA National Institute of Transparency, Access to Information, and Protection of Personal Data (INAI) issued a guide for implementing management systems for the security of personal data (INAI, 2015[79]). It provides direction to controllers and processors for the creation of data management systems/accountable systems that can be used to ensure data stay secure.

Canada's Federal Bill C-27, the Digital Charter Implementation Act 2022, seeks to amend the Personal Information Protection and Electronic Documents Act (PIPEDA) and other acts, as well as enact the Consumer Privacy Protection Act (CPPA), among others. Under the proposed CPPA, data controlling organisations must protect personal information through physical, organisational and technological security. The level of protection from those safeguards must be proportionate to the sensitivity of the information (House of Commons [Canada], 2022[78]). This continues requirements in force with the Personal Information Protection and Electronic Documents Act and remains relevant for encouraging the use of PETs. The bill also includes the Artificial Intelligence and Data Act that would detail required measures to safeguard data and provide a pathway to compliance with regulations. It would also create a new AI and Data Office to support the effort.

The Australian Privacy Principle (APP) 11 requires entities covered by the Privacy Act 1988 to take reasonable steps to protect personal information from misuse, interference and loss, as well as from unauthorised access, modification or disclosure. It does not contain any specific requirements for PETs except that they meet the standard of APP 11 if implemented.

Norway's Data Protection Authority worked with security professionals and software developers to help organisations understand and comply with the requirement of data protection by design and by default in Article 25 of the GDPR. They identified seven activities as part of a continual process to ensure adherence to DPbDD: training, requirements, design, coding, testing, release and maintenance (Datatilsynet, 2017[80]).

Japan's Guidelines on the Act on the Protection of Personal Information Guidelines includes a question-and-answer section that may apply to the use of encrypted data processing tools even though they do not expressly refer to PETs (PPC, n.d.[81]). Under the section of incidents to be reported, question number 6-16[22] is asked and answered related to encrypted personal data that have been or may have been leaked:

> *Answer (6-16): In order to fall under "cases where advanced encryption or other measures are taken for personal data which was or could have been leaked, etc." which do not have to be reported, in light of the technical level at the time of the incident, it is necessary to take technical measures such as encryption that*

> *would make it difficult for a third party to read it, and ensure that the means to make information readable by the technical measures are properly managed. Technical measures such as encryption, which makes it difficult for a third party to read it, include cryptographic techniques, such as those listed in the CRYPTREC Code List or ISO/IEC 18033, which have been verified to be secure by an appropriate evaluation body, and they must be used and implemented appropriately. Means to make information readable by technical measures such as encryption are properly managed, if (i) measures for separating encrypted information from decryption keys and preventing leakage of decryption keys have been taken, (ii) functions for deleting encrypted information or decryption keys with remote operations have been prepared, or (iii) decryption keys are designed to be not usable by third parties.*

In Israel, Article 10(a) of the Protection of Privacy Regulations (Data Security) 5777-2017, stipulates that in systems of a database under medium or high security level, an automatic recording mechanism is mandatory to enable monitoring access to the database systems, including all the following data: user identity, date and time of access attempt, system component to which the access was attempted, access type, its scope, and whether access was granted or denied.

4.1.5. Accountability requirements

PETs are generally considered helpful for organisations to implement the accountability principle, according to which "a data controller should be accountable for complying with measures which give effect to the [OECD Privacy Guidelines' Basic] Principles" (OECD, 2013[7]).

GDPR's Article 28 about data processors who receive data and processing instructions from data controllers' states:

> *Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. (European Union, 2016[14])*

Mexico's General Data Law defines the responsibilities of data controllers (Article 16) and requires that the responsible party complies *by default* with the obligations of the law (Article 30). Regardless of the type of system on which personal data are hosted or the type of processing applied, the data controller must establish administrative, physical and technical security measures to protect personal data. Specifically, the measures need to protect against damage, loss, alteration, destruction or unauthorised use, access to, or processing, and must ensure their confidentiality, integrity and availability (Article 31). Any actions related to personal data processing also must be documented and kept in a management system (Article 34).

4.1.6. Regulatory mandates

The assessment of the replies to the PET questionnaire shows that public bodies promote PETs within the framework of their missions, including through positive obligations. For instance:

In France, the CNIL has a statutory duty to promote the use of PETs, in particular data encryption technologies, by virtue of the Law No. 2016-1321 of October 7, 2016, for a Digital Republic.

In 2020, the Treasury Board of Canada Secretariat launched the Policy on Service and Digital, which outlines the need for privacy protection (see section 4.3.2) (TBC, 2019[82]). The policy states that deputy ministers are responsible for "ensuring that privacy is addressed in the context of any plan or strategy to manage departmental information or data." While this does not explicitly refer to PETs, it does apply to any plans or initiatives that the government of Canada may implement, including plans to adopt new technology (which may include PETs).

Korea’s Personal Information Protection Act does not include explicit regulations on PET use, but two provisions apply to PETs. More specifically Article 7-8 No. 7 stipulates that “(s)upport and dissemination of technology development related to personal information protection” falls under the jurisdiction of the Personal Information Protection Commission.

4.2. Measures to foster innovation in and with PETs

A wide variety of policy initiatives on PETs is underway across OECD countries. The assessment of the responses to the PET Questionnaire show that countries are promoting innovation in and with PETs through: (i) research and technology development, (ii) adoption of secure data processing platforms, (iii) certification of trusted PETs, (iv) innovation contests, (v) regulatory sandboxes and (vi) deployment of digital identity solutions. These initiatives are complemented by private sector initiatives aimed at promoting the adoption of PETs (Box 3).

Box 3. Selected private sector initiatives promoting the adoption of PETs

The Royal Society’s Privacy Enhancing Technologies Programme

The Privacy Enhancing Technologies Programme of the Royal Society, one of the United Kingdom’s major national academies, “aims to investigate the potential for PETs in maximising the benefit and reducing the harms associated with data use.” (Royal Society, 2023[16]) Since its initial (2019[15]) report, the Royal Society commissioned and published multiple reports on PETs including on synthetic data (Jordon et al., 2022[83]), assurance schemes and standards (Georgia Iacovou and Thwaite, n.d.[84]), and market readiness, enabling and limiting factors of PETs in the public sector in the United Kingdom (ODI, 2022[85]).

Its most recent (2023[86]) report on “the role of Privacy Enhancing Technologies in data governance and collaborative analysis”, undertaken in close collaboration with the Alan Turing Institute, “considers the potential for PETs to revolutionise the safe and rapid use of sensitive data for wider public benefit”. It addresses the following questions in particular: (i) How can PETs support data governance and innovative data uses for public good? (ii) What are, and how to address, the primary barriers and enabling factors around the adoption of PETs? And (iii) how might PETs be factored into frameworks for assessing and balancing risks and benefits? (Royal Society, 2023[16])

The Open Loop Experimental Governance Program

Open Loop is a global programme initiated and supported by Meta to connect policymakers and businesses with the aim to co-create policy prototypes and test new and different approaches to laws and regulations for effective and evidence-based policies around AI and other emerging technologies.

In September 2022, Open Loop launched a new policy prototyping programme intended to guide and enable companies in Uruguay and beyond (e.g. Brazil) to leverage and apply PETs with the objective to “help de-identify data and mitigate privacy-related risks, including in AI systems and in the context of the metaverse” (Open Loop, 2022[87]). In so doing the programme aims to incentivise companies to develop and adopt PETs while gathering participants' experience in implementing the developed policy prototypes, and testing their “clarity, effectiveness and actionability” (Open Loop, 2022[87]).

In Uruguay, the programme is led by a consortium including the Meta Open Loop team and the Eon Resilience Lab of C Minds, in collaboration with Uruguay’s e-government agency (“Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento”) and Uruguay’s privacy enforcement authority (“Unidad Reguladora y de Control de Datos Personales”).

4.2.1. Research and development

The Office of the Privacy Commissioner of Canada's (OPC) Contributions Program funds independent privacy research and related knowledge translation initiatives. Applicants are encouraged to propose projects that generate new ideas, approaches, and knowledge about privacy. These projects can help organisations better safeguard personal data and individuals make more informed decisions about protecting their privacy. The Contributions Program was created in 2004 to: (i) support independent, non-profit research on privacy; (ii) further privacy policy development; and (iii) promote the protection of personal data in Canada. The OPC issues an annual call for proposals, usually in the fall. The OPC has specifically called for proposals related to PETs in the past and has made financial contributions in the past to such studies. (OPC, n.d.[88])

The Scientific and Technological Research Council of Türkiye (TÜBİTAK) offers research entities in Türkiye a variety of over 50 grant-based support mechanisms, which are differentiated based on the needs of researchers in the private and public sectors, including entrepreneurs and scholars. These mechanisms are designed to support R&D, innovation, and entrepreneurship in the country with PETs being a focus area, especially in relation to big data, data analytics, the Internet of Things, digital security, cloud computing and software development. These initiatives are complemented by Türkiye's National AI Strategy, which covers data governance and related topics including PETs. In this context, the TÜBİTAK Artificial Intelligence Institute also has been conducting efforts to promote the implementation of PETs.

In the United Kingdom, the Department for Business, Energy and Industrial Strategy is funding a project entitled "PETs for Public Good". As part of this project, the ICO is running a series of workshops with a range of organisations in the health sector (which are both using and not using PETs), as well as academics, researchers, and legal and data protection experts. Together, they learn how PETs can facilitate safe, legal and valuable data sharing in health and what is needed to help organisations use these technologies. The ICO will use conclusions of the workshops to inform its updated guidance on PETs, as well as to outline solutions that enable safe and lawful data sharing in sectors beyond health care.

The Data Science Campus of the United Kingdom Office for National Statistics is undertaking research on synthetic data. In 2019, it produced a report that proposed a synthetic data generation system to support data processing and analysis in cases where real data are sensitive (e.g. identifiable personal data, medical records, defence data) (Kaloskampis, 2019[89]). Current research focuses on applying synthetic data to enable data access, focusing on methods with enhanced privacy guarantees (such as Differential Privacy). In collaboration with researchers from the Alan Turing Institute, the ONS Data Science Campus has created SynthGauge – a Python library that provides a framework for evaluating the utility and privacy of synthetic datasets (Daniels, 2022[90]). It will enable researchers to evaluate synthetic data sets and make informed decisions before putting them to use.

The United Kingdom's Behavioural Insights Team (BIT) has also investigated the potential of synthetic data to support and accelerate public policy research. It has produced a user guide to support researchers generate low-fidelity synthetic data. BIT and the Administrative Data Research UK (ADR UK) are also engaging the ONS on how to integrate this approach with the ONS Secure Research Service and the forthcoming ONS Integrated Data Service. They foresee a central platform where researchers can browse synthetic data sets (BIT, 2 March 2022[91]).

In the United States, research and development (R&D) related to PETs is supported by research-funding agencies across the US government. Notably, the National Science Foundation, National Institute for Standards and Technology, National Institutes of Health, Department of Energy, Department of Veterans Affairs, Centers for Disease Control and Prevention and the Defense Advanced Research Projects Agency support research on PETs. External research is primarily conducted in academic or non-profit settings rather than to develop commercial PET solutions.

The US National Strategy for Privacy Preserving Data Sharing and Analytics is being developed under the auspice of the White House Office of Science and Technology Policy (OSTP). It aims to enable researchers, physicians and others with permitted access to gain insights from sensitive data without accessing the data. OSTP stresses that, to date, PETs have not achieved widespread adoption due to a variety of factors. These include the need for more R&D, limited technical expertise, perceived and possible risks, financial cost and the lack of generalisable solutions (White House [United States], 2022[4]).

In June 2022, Singapore announced the launch of the Digital Trust Centre to lead R&D in trust technologies, and support talent development in this space. The Centre is funded by an SGD 50 million investment from the InfoComm Media Development Authority (IMDA) and National Research Foundation (NRF) under the Research, Innovation and Enterprise (RIE) 2025 plan. Hosted by the Nanyang Technological University, Singapore, the Centre is a national effort to focus on four key areas of trust technologies. To achieve this, DTC will embark on the following:

- Trust Tech Research to enable institutes of higher learning and research institutes to pursue research excellence in trust technologies and drive local and international collaborations
- Trust Tech Innovations to encourage academia and enterprises to co-develop and mature research ideas into market-ready solutions
- a new sandbox environment to enable businesses to experiment with trust technologies to alleviate challenges with data sharing
- deepened local capabilities to nurture 100 R&D talents in digital trust.

Also in Singapore, the Singapore Centre for Research in Innovation, Productivity and Technology is a multidisciplinary research centre funded by a USD 15.3 million grant from IMDA and the NRF. The Centre focuses on research, development, application and transition of technology towards scalable and customised privacy-preserving technologies aligned with national priorities of Singapore in the Services and Digital Economy of RIE 2020 framework. The Centre specialises in "privacy-preserving technologies", which aim to "preserve individual privacy while allowing maximum value and insight to be extracted, while enabling organisations to carry out data mining, analysis and sharing, in compliance with data protection regulation enacted in various jurisdictions."

4.2.2. Secure data processing platforms

OpenSAFELY is a secure analytics platform developed in the United Kingdom in response to the COVID-19 pandemic, enabling researchers to analyse millions of patients' electronic health records. It is an open-source secure analytics platform running across the full pseudonymised primary care records of 55 million patients (more than 95% of the UK population). As such, it allows live analysis of patient records by trusted analysts based anywhere in the world without providing access to these potentially disclosive pseudonymised records. This is done by supporting remote computation directly inside secure data centres and cloud environments executed with code developed using dummy datasets.[23]

The UK National Health Service (NHS) has built a system for linking patient data held across different NHS domains. To protect patient confidentiality, identifiers (such as a patient's NHS number) are pseudonymised through tokenisation. For additional security, the tokenisation differs between different NHS domains. Linking data about a patient held in two domains first requires removing the tokens, which would expose personal information. To avoid this, a partially HE enables data to be linked without revealing the underlying raw identifiers. The NHS Digital/Privitar project uses HE and de-identification techniques.

The UN Committee of Experts on Big Data created the UN Privacy Enhancing Technologies Lab (UN PET Lab) to investigate adoption of PETs within the community of official statistics. The lab seeks to demonstrate that PETs can make fully compliant data sharing between organisations possible (United Nations, 2022[92]; 2023[93]).

4.2.3. Certification of trusted PETs

The Japanese government has studied the use of personal data trust banks to promote distribution and use of personal information in a way that both individuals and companies can feel secure. A personal data trust bank is a business delegated by each individual to manage their personal data and provide it to third parties within certain limits agreed to by the individual. Japan's Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry have formulated guidelines for certification of personal data trust banks. Meanwhile, the Information Technology Federation of Japan, a private organisation, certifies business operators based on the guidelines. These trust banks function as a personal data store that is outsourced to a third party.

4.2.4. Innovation contest

Since 2016, the CNIL in collaboration with the French National Institute for Research in Digital Science and Technology (Inria) gives the CNIL-Inria Privacy Award to scientists and researchers to encourage research in the field of data protection and privacy. Papers are mainly selected based on their scientific excellence and their societal impact. It is seen as an "opportunity to raise the scientific community's awareness of data protection issues and the need to develop research projects in this field, particularly in the light of developments brought by the [GDPR], and in particular the new requirements for privacy by design and accountability."

In Mexico, INAI promotes innovation through an annual Transparency Innovation Contest and the Innovation and Good Practices in the Protection of Personal Data Award. In 2022, the theme for the contest is how to "encourage technological systems, applications and platforms that disseminate and generate best practices that strengthen access to public information, transparency and accountability in Mexico." The Award aims "to promote best practices in the protection of personal data, in addition to recognizing, encouraging and promoting the work" of innovative actors.

In July 2019, the Financial Conduct Authority (FCA) in the United Kingdom held a week-long Global Anti-Money Laundering and Financial Crime TechSprint to find better ways of increasing detection and prevention rates of financial crime. The event focused on how PETs can facilitate sharing of information about money laundering and financial crime concerns, while complying with data security laws.[24] This TechSprint was a catalyst to focus the conversation on PETs and anti-financial crime. Numerous activities have built on this work programme, such as the UK-US PETs Challenge Prize (n.d.[94]) (Box 4).[25]

Box 4. The UK-U.S. privacy-enhancing technologies prize challenges

In July 2022, the United Kingdom and the United States governments launched a set of prize challenges to unleash the potential of PETs to combat global societal challenges. The objective is to provide the opportunity to innovators from academia, industry, and the broader public to participate in up to two separate tracks with the option to design one generalised solution that works for both tracks.

The first track seeks to promote the development of PETs that can facilitate privacy-preserving financial information sharing and collaborative analytics to tackle the challenge of international money laundering, by allowing anomalous payments to be identified without compromising the privacy of individuals.[1] The second track of the challenges aims to bolster pandemic response capabilities and strengthen global readiness for ongoing and future public health emergencies by developing privacy-preserving solutions that can forecast an individual's risk of infection.[2]

Competing for cash prizes from a combined prize pool of USD 1.6 million (GBP 1.3 million), innovators are expected to develop privacy-preserving federated learning solutions that enable artificial intelligence models to be trained on sensitive data without organisations having to reveal, share, or combine their raw data. Winning challenge solutions will be showcased at the second Summit for Democracy to be convened in the first half of 2023.

In November 2022, 12 teams from across the United Kingdom and the United States were announced as winners of Phase 1 of the PETs prize challenges. Applications are now open to join so called "red teams", which will test the strength of privacy protections of the proposed solutions in the final phase.

Note: 1. The first track is based on synthetic global transaction data created by SWIFT, the global provider of secure financial messaging services.
2. The second track is based on synthetic dataset created by the University of Virginia's Biocomplexity Institute, a dataset representing a digital twin of a regional population.
Source: (United Kingdom, 2022[95]; United Kingdom, 2022[96])

4.2.5. Regulatory sandboxes and other supportive environments

The CNIL, France's PEA, is providing a sandbox for use of PETS as it follows the development of privacy-friendly use of AI solutions. To support this progress and promote solutions that respect privacy and personal data by design, the CNIL set up a sandbox in 2021 through which selected companies benefit from enhanced support within the sandbox. In 2021, four innovative projects using health data benefited from this enhanced support. For example, as part of this process, the CNIL supported the University Hospital of Lille to implement federated learning methods that were applied to clinical studies. This technique made it possible to train AI models in a distributed way without requiring circulation of data.

In Singapore, on 20 July 2022, IMDA and the Personal Data Protection Commission (PDPC) announced the launch of a PET sandbox to provide a safe environment and testing ground to pilot PET projects (IMDA, n.d.[97]). These projects will help businesses identify the appropriate PET to address their data-sharing objectives and better understand technical limits. Drawing on the lessons from the pilots, IMDA and PDPC plan to gather the learning points in case studies, identify common software tools that can support industry's adoption of PETs and develop policy guidance to set standards and best practices. Use case owners will be required to bring use cases based on three common business objectives. This focus can help future use case owners, as well as enable IMDA and PDPC to develop future regulatory and technological guidance.

Norway has deployed a similar regulatory sandbox for AI and data protection. It makes DPbDD an obligation for innovation of new tech and AI that process personal data. PETs are expected to play a role in the intersection of these two areas.

In the United Kingdom, the ICO's Sandbox targets innovative projects using personal data across all sectors where there is demonstrable public benefit. The ICO's Sandbox allows to support products and services in these areas which utilise personal data in innovative and safe ways. It started operating in July 2019 with PETs being part of the areas of focus since July 2021. The current focus of the Sandbox is on biometrics, including PETs. The ICO's Sandbox has already delivered a project advising on pseudonymised data to tackle financial crime. Three other projects currently in the ICO's Sandbox include an evaluation of PETs such as differential privacy and synthetic data to anonymise personal data and zero knowledge proofs.

4.2.6. Digital identity management

Finland is developing national legislation on digital identification (Ministry of Finance, Finland, n.d.[98]) to enable citizens and foreigners to use digital identification using a state-issued core identity that follows the principles of self-sovereign identities. The new digital identification is planned to be tracking-resistant, which means the issuer cannot track how the digital ID is being used. The new digital ID solution acts as the basis for national implementation of the upcoming natural person EU Digital Identity wallet. The wallet is based on the revised electronic identification, authentication and trust services (eIDAS) regulation. Digital ID and digital wallet solutions are envisioned to improve individuals' control over their personal data. They will also enable PETs, such as selective disclosure, ZKP and data minimisation.

Digital identification in Finland is regulated by the national Act on Strong Electronic Identification and Electronic Trust Services (Government of Finland, 2009[99]) and Finnish Trust Network (FTN) (Traficom, n.d.[100]). eIDAS regulates cross-border use (European Union, 2014[101]). Both FTN and eIDAS enable some PETs, such as pseudonymous identification. However, they are built with federated digital identity technologies. As such, they cannot reduce the ability of identity providers to track use of digital identities. This is one reason why more privacy-preserving capabilities for the use of digital identities are being developed both nationally and within the European Union.

4.2.7. PETs for official statistics

National statistical offices (NSOs) as well as international organisations in charge of the production and dissemination of official statistics are increasingly considering and promoting the adoption of PETs to foster data sharing in line with privacy and personal data protection legislations. (See e.g. United Nations Economic Commission for Europe, 2022[43]; United Nations, 2022[92]; 2023[93]).

This is reflected for instance in the new proposal on "European statistics on population and housing" by the European Commission (2023[102]). This proposal explicitly supports the adoption of PETs "to implement data sharing fully in line with the EU's personal data protection legislation" while "strengthen[ing] the legal basis and encourag[ing] the development of innovative solutions to enable data sharing". In particular, the proposal recommends "the testing and use of privacy enhancing technologies that implement data minimisation by design" and Article 13 (3) in particular proposes that

> *When the data concerned are confidential data …, the sharing of such data shall be allowed and may take place on a voluntary basis provided it is: … (b) based preferably on privacy enhancing technologies that are specifically designed to implement the principles of Regulations (EU) 2016/679 and (EU) 2018/1725, with particular regard to purpose limitation, data minimisation, storage limitation, integrity and confidentiality;*

Recital 30 of the draft further highlights that "data sharing mechanisms based on privacy enhancing technologies that are specifically designed to implement these principles should be preferred over direct data transmission."

5 Conclusions

- PETs are at different stages of development and will likely need to be part of data governance frameworks to ensure they are used properly in line with the associated privacy risks. Many of these tools are still in their infancy and limited to specific data processing use cases.
- Given their innovative nature and high potential, PETs warrant a comprehensive re-evaluation of the application of regulations on data collection and processing. It is important that this re-evaluation focuses on the effective privacy outcome that PETs may contribute to rather than processes of using a particular PET.
- Policy makers, and PEAs in particular, will increasingly need to consider how the use of PETs may impact regulatory assessments under national privacy and data protection frameworks, taking into account the contribution of PETs to privacy protective outcomes.
- PETs will require complementary tools, tests and procedures to ensure they are used safely and in accordance with the law throughout the economy.
- As PETs mature, there will be an increasing need for awareness raising and training to better design, build, implement, use and audit these new technologies.
- Stronger cross-border and cross-sectoral regulatory co-operation will be needed to better consider technological developments on PETs for privacy and data protection.
- To this end, an analysis of concrete use cases of PETs, including but not limited to the use of PETs for facilitating cross-border data flows, may help inform policy discussions, including in respect to the privacy and economic outcomes PETs promise to help achieve.

References

Abowd, J. (2018), *The U.S. Census Bureau Adopts Differential Privacy*, ACM, London United Kingdom, http://dx.doi.org/10.1145/3219819.3226070. [103]

Acquisti, A. et al. (2017), "Nudges for privacy and security: Understanding and assisting users' choices online", *SSRN*, http://dx.doi.org/10.2139/ssrn.2859227. [68]

Apple (2017), "Learning with privacy at scale", Apple, Cuppertino, CA, https://docs-assets.developer.apple.com/ml-research/papers/learning-with-privacy-at-scale.pdf. [37]

Asrow, K. and S. Samonas (2021), *Privacy Enhancing Technologies: Categories, Use Cases and Considerations*, Federal Reserve Bank of San Francisco, CA. [25]

Bayle, A. et al. (2018), "When Blockchain Meets the Right to be Forgotten:Technology Versus Law in the Healthcare Industry", *Proceedings - 2018 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2018*, pp. 788-792, http://dx.doi.org/10.1109/WI.2018.00133. [110]

BIT (2 March 2022), "Accelerating public policy research with easier & safer synthetic data", Behavioural Insights Team blog, https://www.bi.team/blogs/accelerating-public-policy-research-with-easier-safer-synthetic-data/. [91]

Bogdanov, D. et al. (2016), "Students and taxes: A privacy-preserving study using secure computation", *Proceedings on Privacy Enhancing Technologies*, Vol. 2016/3, pp. 117-135, http://dx.doi.org/10.1515/popets-2016-0019. [53]

Bogetoft, P. et al. (2009), "Secure multiparty computation goes live", in *Financial Cryptography and Data Security*, Dingledine, Roger; Golle, Philippe (eds.), Springer, Berlin, Heidelberg, http://dx.doi.org/10.1007/978-3-642-03549-4_20. [54]

Bruno, G. et al. (2018), "Are post-crisis statistical initiatives completed?" Basel", pp. 30-31. [49]

Cargill, S. et al. (2016), "Community-engaged research ethics review: Exploring flexibility in federal regulations", *IRB Ethics and Human Research*, Vol. 38/3, pp. 11-18. [114]

CDEI (n.d.), *PETs Adoption Guide*, https://cdeiuk.github.io/pets-adoption-guide/adoption-guide (accessed on 7 February 2023). [73]

CDEI (n.d.), "Repository of Use Cases", (database), https://cdeiuk.github.io/pets-adoption-guide/repository/ (accessed on 1 December 2022). [74]

CNIL (2018), *Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ?*, https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles (accessed on 30 January 2023). [111]

Daniel, E. and F. Tschorsch (2021), “Towards Verifiable Mutability for Blockchains”, http://dx.doi.org/10.48550/arxiv.2106.15935. [118]

Daniels, O. (2022), “Evaluating synthetic data using SynthGauge”, 9 June, Data Science Campus, Newport, South Wales, United Kingdom, https://datasciencecampus.ons.gov.uk/evaluating-synthetic-data-using-synthgauge/. [90]

Datatilsynet (2017), *Software development with Data Protection by Design and by Default*, https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true (accessed on 5 December 2022). [80]

de Castro, L. et al. (2020), “SCRAM: A Platform for Securely Measuring Cyber Risk”, *Harvard Data Science Review*, Vol. 2/3, http://dx.doi.org/10.1162/99608f92.b4bb506a. [51]

Demmler, D. et al. (2018), “PIR-PSI: Scaling private contact discovery”, *Proceedings on Privacy Enhancing Technologies*, Vol. 2018/4, pp. 159-178, http://dx.doi.org/10.1515/popets-2018-0037. [56]

Drechsler, J. (2021), “Differential Privacy for Government Agencies -- Are We There Yet?”, http://dx.doi.org/10.48550/arxiv.2102.08847. [36]

EDPB (2020), “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”, European Data Protection Board, Brussels, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf. [1]

EDPS (2021), *10 Misunderstandings related to Anonymisation*, European Data Protection Supervisor, Brussels, https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf. [30]

ENISA (2021), *Data Pseudonymisation: Advanced Techniques and Use Cases*, European Union Agency for Cybersecurity, Athens, https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases. [2]

ENISA (2019), *Pseudonymisation techniques and best practices*, European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices (accessed on 30 January 2023). [29]

ENISA (2016), “PETs Controls Matrix: A Systematic Approach for Assessing Online and Mobile Privacy Tools”, European Union Agency for Cybersecurity, Athens, https://www.enisa.europa.eu/publications/pets-controls-matrix. [27]

ENISA (2016), *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*, https://www.enisa.europa.eu/publications/pets. [20]

European Commission (2023), *Proposal for a Regulation of the European Parliament and of the Council on European statistics on population and housing, amending Regulation (EC) No 862/2007 and repealing Regulations (EC) No 763/2008 and (EU) No 1260/2013*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2023:31:FIN (accessed on 9 February 2023). [102]

European Commission (2021), *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*, https://eur-lex.europa.eu/legal- [38]

content/EN/ALL/?uri=COM%3A2021%3A281%3AFIN (accessed on 31 January 2023).

European Data Protection Supervisor (2021), *Is the future of privacy synthetic?*, https://edps.europa.eu/press-publications/press-news/blog/future-privacy-synthetic_en (accessed on 5 December 2022). [33]

European Union (2016), "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 (GDPR)", European Union, Brussels, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679. [14]

European Union (2014), "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", Document 32014R0910, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910. [101]

FATF (2021), *Stocktake on Data Pooling, Collaborative Analytics and Data Protection*, Financial Action Task Force, Paris, https://www.fatf-gafi.org. [50]

Frankle, J. et al. (2018), *Practical Accountability of Secret Processes*, http://dx.doi.org/10.1000/1 (accessed on 2 December 2022). [70]

G7 (2022), *Communiqué Roundtable of G7 Data Protection and Privacy Authorities: Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces*. [6]

Gardner, S. and A. Vittorio (2022), *Blockchain's Forever Memory Confounds EU 'Right to Be Forgotten'*, Bloomber Law, https://news.bloomberglaw.com/privacy-and-data-security/businesses-adopting-blockchain-question-eus-strict-privacy-law (accessed on 30 January 2023). [109]

GenRocket (n.d.), *Test Data Solutions for Financial Services*, https://www.genrocket.com/financial-services/ (accessed on 1 February 2023). [42]

Georgia Iacovou, B. and A. Thwaite (n.d.), "The current state of assurance in establishing trust in PETs", https://royalsociety.org/-/media/policy/projects/data-governance/data- (accessed on 31 January 2023). [84]

Google (2022), *Applying Differential Privacy to Large Scale Image Classification*, http://ai.googleblog.com/2022/02/applying-differential-privacy-to-large.html. [104]

Gorin, J., M. Biéri and C. Brocas (2022), *Demonstration of a privacy-preserving age verification process*, Laboratoir d'Innovation Numérique de la CNIL, https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process (accessed on 1 February 2023). [39]

Government of Finland (2009), *Act on Strong Electronic Identification and Electronic Trust Services*, Government of Finland, https://www.finlex.fi/en/laki/kaannokset/2009/en20090617. [99]

Grubbs, P., T. Ristenpart and V. Shmatikov (2017), *Why Your Encrypted Database Is Not Secure*, https://summerschool-croatia.cs.ru.nl/2017/slides/Why%20your%20encrypted%20database%20is%20not%20secure.pdf (accessed on 25 November 2022). [105]

Hard, A. et al. (2018), *Federated Learning for Mobile Keyboard Prediction*, https://research.google/pubs/pub47586/ (accessed on 29 September 2022). [58]

Harmon, A. (2010), "Indian Tribe Wins Fight to Limit Research of Its DNA", *The New York Times*, https://www.nytimes.com/2010/04/22/us/22dna.html (accessed on 31 January 2023). [115]

Harvard University (n.d.), *Differential Privacy | Harvard University Privacy Tools Project*, https://privacytools.seas.harvard.edu/differential-privacy (accessed on 5 December 2022). [108]

Hausman, D. (2008), "Protecting groups from genetic research", *Bioethics*, Vol. 22/3, pp. 157-165, http://dx.doi.org/10.1111/j.1467-8519.2007.00625.x. [113]

Hausman, D. (2007), "Group risks, risks to groups, and group engagement in genetics research", *Kennedy Institute of Ethics journal*, Vol. 17/4, pp. 351-369, http://dx.doi.org/10.1353/KEN.2008.0009. [112]

Hawkins, A. (2021), *Welcome to Simulation City, the virtual world where Waymo tests its autonomous vehicles*, The Verge, https://www.theverge.com/2021/7/6/22565448/waymo-simulation-city-autonomous-vehicle-testing-virtual (accessed on 1 February 2023). [40]

Henriksen-Bulmer, J. and S. Jeary (2016), "Re-identification attacks – A systematic literature review", *International Journal of Information Management*, Vol. 36/6, Part B, pp. 1184-1192, http://dx.doi.org/10.1016/j.ijinfomgt.2016.08.002. [45]

House of Commons [Canada] (2022), *BILL C-27*, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading (accessed on 5 December 2022). [78]

ICO (2022), "Chapter 5: Privacy-enhancing technologies (PETs)", Information Commissioner's Office, London, https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf. [5]

ICO (2022), "ICO Call for Views: Anonymisation, Pseudonymisation and Privacy Enhancing Technologies Guidance", Information Commissioner's Office, London, https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/. [72]

IMDA (2022), "ATxSG 2022 'Trust in Data' Roundtable Report on Key Insights". [17]

IMDA (2022), *Invitation to participate in the Privacy Enhancing Technology Sandbox*, Infocomm Media Development Authority, https://www.imda.gov.sg/-/media/Imda/Files/Programme/PET-Sandbox/PET-Sandbox-CFP.pdf (accessed on 1 February 2023). [22]

IMDA (n.d.), "IMDA and PDPC launch Singapore first privacy enhancing technologies sandbox as they mark decade-long effort of strengthening public trust", 10 July, News Release, InfoComm Media Development Authority, https://www.imda.gov.sg/news-and-events/Media-Room/. [97]

INAI (2015), *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, [Guide to implement a Personal Data Security Management System], National Institute for Transparency, Access to Information Protection of Personal Data, Ocoyoacac, Mexico, https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf. [79]

Ion, M. et al. (2020), "Private intersection-sum protocols with applications to attributing aggregate [57] ad conversions", presented to 2020 IEEE European Symposium on Security and Privacy (EuroS\&{P}), https://eprint.iacr.org/2019/723.pdf.

Isaak, J. and M. Hanna (2018), "User data privacy: Facebook, Cambridge Analytica, and Privacy Protection", *Computer*, Vol. 51/8, pp. 56-59, http://dx.doi.org/10.1109/MC.2018.3191268. [10]

Janssen, H. et al. (2020), "Decentralized data processing: personal data stores and the GDPR", *International Data Privacy Law*, Vol. 10/4, pp. 356-384, http://dx.doi.org/10.1093/idpl/ipaa016. [60]

Jiang, X., X. Zhou and J. Grossklags (2022), "Comprehensive Analysis of Privacy Leakage in Vertical Federated Learning During Prediction", *Proceedings on Privacy Enhancing Technologies*, Vol. 2022/2, pp. 263-281, http://dx.doi.org/10.2478/popets-2022-0045. [59]

Jordon, J. et al. (2022), "Synthetic Data-what, why and how?", http://dx.doi.org/10.48550/arXiv.2205.03257 (accessed on 31 January 2023). [83]

Kaloskampis, I. (2019), "Synthetic data for public good", 21 February, Data Science Campus, Newport, South Wales, United Kingdom, https://datasciencecampus.ons.gov.uk/projects/synthetic-data-for-public-good/. [89]

Kenny, S. (2008), "An introduction to privacy enhancing technologies", 1 May, International Association of Privacy Professionals, Portsmouth, NH, https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies. [23]

Koens, T. (19 January 2021), "Multiparty computation threshold signing in practice: Bringing security to our customers", ING Blog, https://medium.com/ing-blog/multiparty-computation-threshold-signing-in-practice-bringing-security-to-our-customers-f2d63b912bca. [64]

Lapets, A. et al. (2019), "Role-based ecosystem for the design, development, and deployment of secure multi-party data analytics applications", *2019 IEEE Cybersecurity Development (SecDev)*, pp. 129-140, http://dx.doi.org/10.1109/SecDev.2019.00023. [52]

Léautier, A. (2022), *[Données synthétiques] - Dis papa, comment on fait les données ? 1/2 | LINC*, https://linc.cnil.fr/donnees-synthetiques-dis-papa-comment-fait-les-donnees-12 (accessed on 1 February 2023). [32]

Ministry of Finance, Finland (n.d.), "Digital Identity", webpage, https://vm.fi/en/digital-identity (accessed on 1 December 2022). [98]

Montjoye, Y. et al. (2015), *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*, European Union Agency for Cybersecurity, Athens, https://data.europa.eu/doi/10.2824/641480. [26]

Narayanan, A. and E. Felten (2014), "No silver bullet: De-identification still doesn't work", *White Paper*, No. 8, 9 July, Princeton University. [44]

NIST (2020), *Nist Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0*, National Institute of Standards and Technology, US Department of Commerce, http://dx.doi.org/10.6028/NIST.CSWP.01162020. [28]

OCP (12 April 2021), "Privacy tech-know blog: Privacy enhancing technologies for businesses", OCP blog, https://priv.gc.ca/en/blog/20210412/. [3]

ODI (2022), *Privacy Enhancing Technologies: Market Readiness, Enabling and Limiting Factors in the UK public sector*, https://royalsociety.org/-/media/policy/projects/privacy-enhancing- [85]

technologies/Privacy-Enhancing-Technologies-Market-Readiness-Enabling-and-Limiting-Factors.pdf (accessed on 31 January 2023).

OECD (2022), *Recommendation of the Council on Blockchain and Other Distributed Ledger Technologies*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0470 (accessed on 5 December 2022). [63]

OECD (2022), "Responding to societal challenges with data: Access, sharing, stewardship and control", *OECD Digital Economy Papers*, No. 342, OECD Publishing, Paris, http://dx.doi.org/10.1787/2182ce9f-en. [61]

OECD (2021), "Mapping data portability initiatives, opportunities and challenges", *OECD Digital Economy Papers*, No. 321, OECD Publishing, Paris, http://dx.doi.org/10.1787/a6edfab2-en. [65]

OECD (2021), *Report on the Implementation of the Recommendation of the Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris. [8]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, http://dx.doi.org/10.1787/276aaca8-en. [9]

OECD (2018), *Blockchain Primer*, OECD, https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf. [116]

OECD (2016), *Recommendation of the Council on Health Data Governance*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433 (accessed on 13 March 2022). [76]

OECD (2013), *OECD Privacy Framework*, OECD, Paris, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [12]

OECD (2013), "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", No. OECD/Legal 0188, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [7]

OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k8zq92vdgtl-en. [13]

OECD (2010), *30 years After: The impact of the OECD Privacy Guidelines*, OECD, Paris, France. [11]

OECD (2005), *Synthetic data*, https://stats.oecd.org/glossary/detail.asp?ID=7003. [31]

OECD (2002), *Inventory of Privacy-Enhancing Technologies (PETs)*, OECD, Paris, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/reg%282001%291/final. [18]

OECD (1998), *Ministerial Declaration on the Protection of Privacy on Global Networks*, Abrogated on: 18/11/2016, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0301 (accessed on 5 December 2022). [107]

OPC (2022), *Privacy Tech-Know blog: When what is old is new again – The reality of synthetic data*, OPC blogger, https://priv.gc.ca/en/blog/20221012/?id=7777-6-493564 (accessed on 5 December 2022). [34]

OPC (2021), *Privacy Tech-Know blog: Privacy Enhancing Technologies for Businesses*, https://www.priv.gc.ca/en/blog/20210412/ (accessed on 5 December 2022). [71]

OPC (2017), *Privacy Enhancing Technologies – A Review of Tools and Techniques*, Office of the Privacy Commissioner of Canada, Ottawa, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/. [21]

OPC (n.d.), *Funding for privacy research and knowledge translation*, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/ (accessed on 5 December 2022). [88]

Open Loop (2022), *Privacy Enhanging Technologies (PETs)*, https://openloop.org/programs/open-loop-uruguay-program/ (accessed on 31 January 2023). [87]

Ozbek Cittone, S. and B. Aytaç (2019), *Deletion, Destruction Or Anonymization Of Personal Data - Data Protection*, https://www.mondaq.com/turkey/data-protection/790226/deletion-destruction-or-anonymization-of-personal-data (accessed on 9 February 2023). [119]

Pence, E. (2022), “Beyond cryptography: Deniable privacy for secure data aggregation”, MA thesis, Massachussets Institute of Technology, Cambridge, MA. [48]

Politou, E. et al. (2021), “Blockchain Mutability: Challenges and Proposed Solutions”, *IEEE Transactions on Emerging Topics in Computing*, Vol. 9/4, pp. 1972-1986, http://dx.doi.org/10.1109/TETC.2019.2949510. [117]

PPC (n.d.), “Questions and answers”*, Guidelines on the Act on the Protection of Personal Information Guidelines*, Personal Information Protection Commission, Tokyo, https://www.ppc.go.jp/personalinfo/faq/APPI_QA/#q6-16. [81]

Reeves, M. et al. (2020), “Taming complexity”, *Harvard Business Review* January-February, https://hbr.org/2020/01/taming-complexity. [67]

Rivest, R. et al. (2020), “The PACT protocol specification”, Private Automated Contact Tracing Team, Masschussetts Institute of Technology, Cambridge, MA. [55]

Rocher, L., J. Hendrickx and Y. de Montjoye (2019), “Estimating the success of re-identifications in incomplete datasets using generative models”, *Nature Communications*, Vol. 10/1, p. 3069, http://dx.doi.org/10.1038/s41467-019-10933-3. [46]

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 (accessed on 31 January 2023). [86]

Royal Society (2023), *Privacy Enhancing Technologies*, https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/ (accessed on 31 January 2023). [16]

Royal Society (2019), *Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in data analysis*, Royal Society, London, https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf. [15]

Sacolick, I. (2022), “Use synthetic data for continuous testing and machine learning”, *InfoWorld*, https://www.infoworld.com/article/3649055/use-synthetic-data-for-continuous-testing-and- [41]

machine-learning.html (accessed on 1 February 2023).

Seničar, V., B. Jerman-Blažič and T. Klobučar (2003), "Privacy-enhancing technologies – approaches and development", *Computer Standards & Interfaces*, Vol. 25/2, pp. 147-158, http://dx.doi.org/10.1016/S0920-5489(03)00003-5. [19]

Stadler, T., B. Oprisanu and C. Troncoso (2020), "Synthetic Data -- Anonymisation Groundhog Day", *Proceedings of the 31st USENIX Security Symposium, Security 2022*, pp. 1451-1468, http://dx.doi.org/10.48550/arxiv.2011.07018. [35]

Tang, J. et al. (2017), "Privacy Loss in Apple's Implementation of Differential Privacy on MacOS 10.12". [47]

TBC (2019), "Policy and Service on Digital", webpage, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603 (accessed on 1 December 2022). [82]

Traficom (n.d.), "Electronic Identification", webpage, http://berturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification. (accessed on 1 December 2022). [100]

Treasury Board of Canada Secretariat (2020), "Policy on Service and Digital", p. 21. [106]

UK-US Prize Challenges (n.d.), *Privacy Enhancing Technologies Prizes*, website, https://petsprizechallenges.com/ (accessed on 1 December 2022). [94]

United Kingdom (2022), *UK and US launch innovation prize challenges in privacy-enhancing technologies to tackle financial crime and public health emergencies*, https://www.gov.uk/government/news/uk-and-us-launch-innovation-prize-challenges-in-privacy-enhancing-technologies-to-tackle-financial-crime-and-public-health-emergencies (accessed on 30 January 2023). [95]

United Kingdom (2022), *Winners announced in first phase of UK-U.S. privacy-enhancing technologies prize challenges*, https://www.gov.uk/government/news/winners-announced-in-first-phase-of-uk-us-privacy-enhancing-technologies-prize-challenges (accessed on 30 January 2023). [96]

United Kingdom (2018), *Data Protection Act*. [75]

United Nations (2022), "What is the UN PET Lab and why is it important?", *53rd Session of the United Nations Statistical Commission Side Event*, 8 February, UN Big Data, https://unstats.un.org/bigdata/events/2022/unsc-un-pet-lab/index.cshtml. [92]

United Nations Committee of Experts on Big Data and Data Science for Official Statistics (ed.) (2023), *The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics*, United Nations, New York, https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf (accessed on 14 February 2023). [93]

United Nations Economic Commission for Europe (2022), *Synthetic Data for Official Statistics: A Starter Guide*, United Nations, Geneva, https://unece.org/sites/default/files/2022-11/ECECESSTAT20226.pdf (accessed on 1 February 2023). [43]

United States Congress (1996), "Health Insurance Portability and Accountability Act", webpage, https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996 (accessed on 29 September 2022). [77]

WEF (2019), *The Next Generation of Data Sharing in Financial Services*, World Economic Forum, Cologny, Switzerland. [24]

White House [United States] (2022), *Request for Information on Advancing Privacy-Enhancing Technologies*, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies (accessed on 29 September 2022). [4]

Zhou, J. et al. (2021), "A survey on federated learning and its applications for accelerating industrial Internet of Things", *arXiv*, Vol. 2104.10501 [cs.DC], https://doi.org/10.48550/arXiv.2104.10501. [62]

Zundel, B. et al. (2022), *Engineering Privacy for Verified Credentials: In Which We Describe Data Minimization, Selective Disclosure, and Progressive Trust*, W3C, https://w3c-ccg.github.io/data-minimization/ (accessed on 31 January 2023). [66]

Zyskind, G., O. Nathan and A. Sandy Pentland (2015), *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, http://github.com/google/leveldb. [69]

Notes

[1] The OECD held a ministerial conference in Ottawa, Canada in 1998 on realizing the potential of global electronic commerce. In international policy circles, the conference represented one of the first large-scale conferences devoted to Internet policy. The conference conclusions produced nearly 25 years ago in 1998 specifically called on governments to "encourage the use of privacy-enhancing technologies". (OECD, 1998[107])

[2] For discussion on the risk of group harm see (Hausman, 2007[112]; Hausman, 2008[113]; Harmon, 2010[115]; Cargill et al., 2016[114]).

[3] See Recital 26 of the European Union (2016[14]) General Data Protection Regulation (GDPR) ("Not Applicable to Anonymous Data") which states that "(t)he principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

[4] A set is fully synthetic when the data it contains has been generated entirely by a model. In practice, the characteristics of the real data set (such as its statistical distribution) are extracted, and then the synthesis set is generated in order to reproduce these characteristics while introducing randomness.

[5] This includes data sets where only some of the variables have been generated according to the previous process. This protocol can be applied to a set containing, for example, particularly identifying data such as age or address.

[6] A hybrid data set will have been generated from the real set and a fully synthetic set to better represent the specifics of the real set. To do this, it is possible, for example, for each of the real points, to select the closest point in the synthetic set: this will make it possible to reproduce certain special cases of the source set without directly using the real data.

[7] One such attack is what is known as a "membership inference" attack. "This is where an attacker attempts to learn whether an individual's record was present in the source data by analyzing properties of the synthetic data. Sometimes even membership in a data set can reveal sensitive information. For example, if a data set is specific to individuals with dementia or HIV, then the mere fact that an individual's record was included in it would reveal personal information about them." (OPC, 2022[34])

[8] As Harvard University's Privacy Tools project puts it: "The guarantee of a differentially private algorithm is that its behavior hardly changes when a single individual joins or leaves the dataset — anything the algorithm might output on a database containing some individual's information is almost as likely to have come from a database without that individual's information. … This gives a formal guarantee that individual-level information about participants in the database is not leaked." (Harvard University, n.d.[108])

[9] See for example (Apple, 2017[37]; Abowd, 2018[103]; Google, 2022[104]).

[10] A popular example can be seen on the website http://www.thispersondoesnotexist.com/ (accessed 01 December 2022) which generates synthetic photos of people.

[11] See for example Grubbs, Ristenpart and Shmatikov (2017[105]) presenting on why encrypted databases are not secure.

[12] This is also true for more than one observation. For example, where two parties use MPC to compute e.g. the maximum of their salaries, the party with the lower salary can learn that of the other party directly from the MPC output.

[13] For example, Frankle et al. (2018[70]) present a DLT enabled accountability system which could be used to improve the accountability of electronic surveillance practices characterised by an "opaque process often involving cases sealed from public view and tech companies subject to gag orders against informing surveilled users". The "system is centered around a publicly visible, append only ledger where the various entities involved in the electronic surveillance process [judges, law enforcement agencies, and companies] can post information[, while] the public can view and verify all data posted to the ledger".

[14] It should be noted here that DLTs may differ in terms of their characteristics including the degree of their mutability. (OECD, 2018[116]; Daniel and Tschorsch, 2021[118]; Politou et al., 2021[117])

[15] It is often quoted in this context that DLTs' characteristics, and especially their immutability, put at risk the GDPR's right to erasure (Art. 17 and 19 GDPR), also known as the right to be forgotten. (Gardner and Vittorio, 2022[109]) How to reconcile the DLTs' characteristics properties with the law have been discussed and promising approaches proposed however. (CNIL, 2018[111]; Bayle et al., 2018[110])

[16] Appropriate anonymisation and/or pseudonymisation tools can for exampe be used when generating immutable audit trail to ensure that audit trails do no make it possible to track what and how data are accessed by individuals.

[17] The Norwegian government has highlighted the role PETs can play in helping older data systems (that pre-date the GDPR) to comply with Article 25 which applies retroactively to all systems.

[18] "The Guideline urges the data controllers to provide the conditions below: It shall not be possible for the anonymized data group to be de-anonymized through combination of another data group, It shall not be possible for one or more values to constitute a whole single meaningful data and It shall not be possible for anonymized data in a data group to be combined into an assumption or conclusion about a person's identity." (Ozbek Cittone and Aytaç, 2019[119])

[19] In 2020, the Treasury Board of Canada Secretariat (TBS) launched the Policy on Service and Digital, which outlines the need for Privacy Protection (Treasury Board of Canada Secretariat, 2020[106]). The Policy states that deputy ministers are responsible for "ensuring that privacy is addressed in the context of any plan or strategy to manage departmental information or data." (Treasury Board of Canada Secretariat, 2020, section 4.3.2.6[58]). While this does not explicitly refer to PETs, it does apply to any plans or initiatives that the Government of Canada may implement, including plans to adopt new technology (which may include PETs).

[20] Article 10 (2) of Türkiye's By-Law on Erasure, Destruction or Anonymization of Personal Data further specifies that "[t]o anonymize the personal data, personal data shall be rendered impossible to relate to identified or identifiable person, even through using appropriate techniques in respect of the recording medium and relevant field of activity …".

[21] Article 5.1 of the Circular states the need to avoid the use of identifiable data for purposes other than those for which they were provided. Articles 5.2-5.3 stipulate that without consent or authorisation by law to use personal identifiable data, secondary use of health data can only be done with anonymised data, provided that anonymisation is completed before access is given to the personal data. Even with regard to uses authorised by law, anonymised data should be preferred over identified data for secondary use.

[22] "Question (6-16): What does it mean by "cases where advanced encryption or other measures are taken for personal data which was or could have been leaked, etc.?" (PPC, n.d.[81])

[23] The real-time analysis enabled by the platform has been critical to the response to COVID-19 through early identification of risk factors.

[24] More than 140 participants at the FCA's offices and at a satellite office in Washington came together to develop solutions using PETs.

[25] See also the work of the Financial Action Task Force (2021[50]) taking stock on "Data Pooling, Collaborative Analytics and Data Protection".