THE GOOD ADVERTISING PROJECT

Privacy-enhancing technologies in the online advertising sector: technical overview and privacy implications

March 2025

Executive summary

The goal of this White Paper is to provide a global overview of privacy-enhancing technologies (PETs) and their growing number of applications, particularly in online advertising, while assessing their impact on privacy.

Over the last couple of decades, digital advertising has become more and more data-intensive, raising privacy concerns due to extensive personal data processing. In the EU, ePrivacy Directive and GDPR constitute the legal pillars of online privacy protection, leading to a system based on consent banners. Although a consent-based system has enabled a certain level of protection, it has also shown its lack of effectiveness due to users' consent fatigue.

The recent developments in privacy-enhancing technologies (PETs), particularly in online advertising, have opened new perspectives to create efficient advertising technologies reducing privacy risks. Among these technologies should be listed anonymization, pseudonymization, homomorphic encryption, trusted execution environments, zero-knowledge proof or even user control tools.

Among the challenges identified to PETs adoption are: the lack of understanding and awareness of the potential of PETs, the lack of industry best-practices, and the lack of official guidance and incentives from lawmakers and authorities.

This White Paper aims at participating to overcome the identified challenges by providing a high level understanding and increasing awareness on PETs. Hopefully, together with other initiatives and efforts from the industry, authorities and lawmakers, this will create the conditions for new standards and best practices, and pave the way for new regulatory frameworks, to promote and incentivize the adoption of PETs in online advertising.

Table of content

Introduction: why promote the development of PETs in digital advertising?

Digital advertising. Digital advertising involves promoting products or services through digital channels such as websites, social media, search engines, and mobile apps. Among various forms of digital advertising (search, social media and classified), display advertising involves the use of text banner, image or video ads on publishers' websites and apps, such as streaming services, online newspapers, large e-commerce platforms. In the early days of digital advertising, display advertising was bought directly from publishers. As the number of publishers selling advertising online increased, programmatic advertising eventually began to replace ad networks as an automated way of buying and selling digital ad space across multiple websites and publishers in real time[1].

Contextual and personalized advertising. Historically, two main approaches to digital display advertising include: (i) contextual advertising adapts to the content seen in real time by the user, without relying on information previously collected[2], and (ii) personalized (behavioral) advertising relies on user's interests to show the most relevant ads, which may be determined using various tracking tools. Among the numerous tracking tools[3], the most historically widespread were:

- **cookies**: small files stored on a device, such as a computer, a mobile device or any other device that can store information, that serve a number of important functions, including remembering users and their previous interactions with a website.[4] "Cookie syncing" enables the data collected by cookies to be consolidated and linked to central identifiers, which are used for advertising purposes. Cookies can be used to collect data about people's browsing history, including the websites or pages they visit and the content they view.[5]
- **tracking pixels**: a hyperlink to a resource, usually an image file, embedded into a piece of content like a website or an email. This pixel usually fulfils no purpose related to the requested content itself; its sole purpose is to automatically establish a communication by the client to the host of the pixel, which would otherwise not have occurred.[6]
- **device fingerprinting**: fingerprints are generated by combining attributes of the user's device or browser with data standardly provided in network requests (e.g. IP address, user agent string, OS version). The permutation of these features is used by

[1] **EU Commission** - Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers – 2023 - Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers - Publications Office of the EU: *"Programmatic advertising is made possible by two key additional layers in the system: 1) Demand-side platforms (DSPs) which enable advertisers and agencies to automate the buying of digital advertising; and 2) Supply-side platforms (SSPs) used by publishers to manage, sell and optimise advertising space (also known as inventory) on their websites, mobile apps and other digital properties in an automated way."*

[2] **IABEurope** – The IAB Europe guide to contextual advertising – July 2021: Regarding contextual advertising - https://iabeurope.eu/wp-content/uploads/IAB-Europe-Guide-to-Contextual-Advertising-July-2021.pdf: *"For example, an ad for running shoes could be placed on a news article about an upcoming marathon, or an ad for laptops on a tech ecommerce site. The idea being that it improves the advertising experience, as the user will only be delivered an ad that is relevant in context of the content they are reading or viewing."*

[3] **EDPB** - Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive – October 7th, 2024 - edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf

[4] **EDPB** – What are cookies? - https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/what-are-cookies_en

[5] **EU Commission** - Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers – 2023.

[6] **EDPB** - Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive – October 7th, 2024.

intermediaries to generate a hash which is used as a non-resettable identifier and database key for that user.[7]

Privacy concerns. Digital advertising has become an increasingly data-driven industry in the past decades. Users' data collected include demographic, interest, intent, location and measurement (impressions, engagement, conversion). They are used for targeting and measuring advertising campaigns and are sometimes tied to common identifiers that enable companies to build up a picture of an individual's behavior across sites, apps, platforms and devices. As personal data processed increased, also did society's awareness of the risks associated to such processing. In parallel, both lawmakers and enforcers have strengthened individual privacy rights. In the EU, 2002 ePrivacy Directive and 2016 General Data Protection Regulation (GDPR) have been the basis of the legal framework to protect privacy and personal data for EU consumers.

Industry significance and privacy awareness. Since the first online banner ad was placed in 1994, the global industry has grown from about €99 million in 1995 to €357 billion in 2021[8]. Particularly, this growing industry has enabled a large number of publishers to create new revenue streams and foster a more diverse and content-driven internet, beginning with online journalism[9]. In the last decade, major actors of the digital advertising industry have taken significant steps to limit access to advertising-related data. For instance, Apple has restricted third-party tracking on its platform. Moreover, Google's Privacy Sandbox aims to bring together different parts of the advertising industry to develop new solutions that are more "privacy-preserving".[10]

Emergence of privacy-enhancing technologies (PETs) applied to online advertising. The recent developments in privacy-enhancing technologies (PETs), particularly applied to online advertising, have opened new perspectives to create efficient advertising technologies reducing the risks to rights and freedoms of personal data processing activity. **PETs is an umbrella term** to designate multiple tools, technologies and techniques used to protect users from cyberattacks, maintain their privacy, strengthen privacy safeguard and in a number of situation, minimize the amount of personal data processed by third parties. So far, key stakeholders observe that among the biggest challenges in PETs adoption are: the lack of understanding and awareness of the potential of PETs, the lack of industry best-practices, and the lack of official guidance and incentives from lawmakers and authorities.

Opportunity to incentivize the development of PETs in online advertising. There is an opportunity for the industry, authorities and lawmakers to work together to create a new regulatory framework, new standards and best practices to promote and incentivize the adoption of PETs in online advertising.

Methodology: a technical approach of PETs and their privacy implications

[7] **EU Commission** - Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers – 2023.

[8] **EU Commission** - Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers – 2023.

[9] **Statista** - Subscriptions and Ads Still Key to Financing Journalism - https://www.statista.com/chart/26594/important-revenue-streams-in-journalism/

[10] **EU Commission** - Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers – 2023.

PETs description based on ENISA's taxonomy. In order to provide a global overview of PETs, this White Paper is based on the European Union Agency for Cybersecurity's (ENISA) taxonomy[11]. This choice is based on (i) the clarity of the broad categories defined by ENISA, easy to understand for non-technical persons, (ii) the relevancy of ENISA approach to articulate PETs with privacy concepts and (iii) the close cooperation between ENISA and European data privacy authorities.

Articulation with privacy concepts. In order to assess why each of these technologies enhance privacy, we have selected key principles arising from ePrivacy Directive[12] and General Data Protection Regulation (GDPR) [13]. These principles, which are particularly relevant to assess the impact of PETs on the protection of privacy and personal data are: data minimization[14]; purpose limitation[15]; storage limitation (duration)[16]; integrity, confidentiality and security[17]; transparency[18] end-user empowerment[19].

Use cases and practical insights. In order to provide an overview of each PET in a way that can be understood by a broad public, a use case is detailed for each PET, as well as practical insights based on information shared by PET developers. Of course, since PETs are constantly evolving, such practical insights are as of the publication date of this white paper, and subject to evolution.

---

[11] **ENISA Report** – Data Protection Engineering – 2022.

[12] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("**ePrivacy Directive**") – Article 1 - *"This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community".*

[13] 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**") – Article 1 - "*This regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*".

[14] **Ireland Data Protection Commission** – Principles of Data Protection - https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection: *"Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means".*

[15] **Ireland Data Protection Commission** – Principles of Data Protection: *"Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data".*

[16] **Ireland Data Protection Commission** – Principles of Data Protection: *"Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed".*

[17] **Ireland Data Protection Commission** – Principles of Data Protection: *"Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".*

[18] **Ireland Data Protection Commission** – Principles of Data Protection: *"The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used".*

[19] End-users must be able to control the way their information and personal data are collected and used. Thus, they must have the opportunity to refuse to have a cookie or a similar advertising technology stored on their terminal equipment (see ePrivacy Directive – Cons. 25) and, under certain conditions, they must be able to object to the processing of their personal data (see GDPR – Article 21). In other words, users must play an active role, not just be passive observers of how their data is used.

Table overview of PETs and their privacy impact

		Data minimization	Purpose &Storage limitation	Integrity and conf. (security)	Transparency & End-User empower
Pseudonymization and Anonymization	Pseudonymization	✓	✓	✓	
	Anonymization (k-anonymity & differential privacy)		✓	✓	
Data masking and privacy-preserving computations	Homomorphic Encryption		✓	✓	
	Secure MPC	✓	✓	✓	
	TEEs		✓	✓	
	Private Information Retrieval	✓		✓	
	Synthetic Data	✓	✓	✓	
Access, communicat. and storage	End-to-end Encryption		✓	✓	
	Proxy & Onion Routing	✓	✓	✓	
	Privacy Preserving Storage		✓	✓	
	Attribute Based Credentials	✓	✓	✓	
	ZKPs	✓	✓	✓	
Transparency, intervenability and user control tools		✓	✓	✓	✓

1. Anonymisation and Pseudonymisation

Before analyzing the concepts of pseudonymization (**1.1.**) and anonymization (**1.2.**) in greater details, it is important to clarify the main difference between these two concepts:

- **Anonymous data** are not considered as personal data, as they do not relate to an identified or identifiable natural person;
- **Pseudonymized data** are personal data, as pseudonymized data can be (re)attributed to a natural person with the use of additional information.

1.1. What is Pseudonymisation and how does it impact privacy?

General explanation. In short, the purpose of pseudonymization is to process data in such a way as to remove potentially identifiable information, in order to prevent the data from being attributed to a unique person. Pseudonymization reduces the risk of identification, but does not totally exclude it, since re-identification remains possible through indirect or additional information[20].

Pseudonymisation can be reached using various techniques, the main ones being as follows[21]:

- **Basic pseudonymisation techniques**: counter, Random Number Generator (RNG), cryptographic hash function, message authentication code (MAC), symmetric encryption ;
- **Advanced pseudonymisation techniques**: asymmetric encryption, ring signatures and group pseudonyms, chaining mode, pseudonyms based on multiple identifiers or attributes, pseudonyms with proof of ownership (ZKP), secure multiparty computations, secret sharing schemes.

How PETs relying on pseudonymization enhance privacy. The benefits of pseudonymisation in terms of privacy protection relate in particular to the following principles:

- **Integrity and confidentiality**, by preventing the data from being attributed to a determined person unless additional information is provided, pseudonymization contributes to user's privacy. Privacy is also strengthened in the event of unlawful access, accidental loss, destruction or damage for instance is necessarily limited;
- **Data minimization**, as the controller performs a detailed analysis of the data collected, and adds complexity to the processing of such data, pseudonymization may lead to a reduction of the overall volume of personal data collected and processed;
- **Purpose limitation**, pseudonymization may be considered in the "purpose compatibility test", especially regarding the consequences of the intended further processing for data subjects or the existence of appropriate safeguards in both the original and intended further processing operations.

---

[20] **OECD** - Emerging Privacy Enhancing Technologies - Current Regulatory and Policy Approaches – 2023: *"Compared to anonymisation, pseudonymisation is a weaker form of deidentification. 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."*

[21] **ENISA** – Data Pseudonymisation: Advanced Techniques & Use Cases – 2021.

Use case: Pseudonymization is used in third-party cookies: by linking a random identifier to a unique browser, only the identifier is stored in a third-party cookie and associated with future ad requests.

Practical insight: Pseudonymisation techniques involve an increase of the cost for re-identification, leading to an improved protection of end-users' privacy. Although pseudonymisation does not offer the same level of protection as anonymisation, it is nonetheless recognised by data protection authorities as an additional safeguard. Practically, combining pseudonymisation with aggregation techniques provides a high level of protection.

1.2. What is Anonymization?

General explanation. For data to be considered anonymous, it must be processed in such a way that it can no longer be used to identify a natural person, "*having regard to all the means "likely reasonably" to be used for identification*"[22]. Anonymisation requires the implementation of an irreversible process which shall resist three main cumulative risks[23]:

- Singling out, which means being able to isolate some or all of the records identifying an individual in the dataset;
- Linkability, which is the ability to link, at least, two records concerning the same data subject or to a group of data subjects;
- Inference, which is the possibility to deduce, with a high degree of probability, the value of an attribute from the values of a set of other attributes. [24]

Among all the techniques that can be used to achieve anonymization, **ENISA's taxonomy has chosen to focus on two main techniques which are cumulative and compatible: k-anonymity (1.2.1) and differential privacy (1.2.2)**.

1.2.1. What is K-Anonymity and how does it impact privacy?

General explanation. K-anonymity is an anonymization method designed to prevent individual identification by ensuring that at least K individuals have the same characteristics. To achieve this, the attribute values (e.g. age, gender, country of birth, etc.) are generalized to an extent such that each individual shares the same value (e.g. age [20-30], [30-40], etc.). The only accessible data would be identical for a multitude of people. This attribute must be sufficiently broad to avoid creating attribute groups too restricted[25][26].

---

[22] **Article 29 data protection working party** - Opinion 05/2014 on Anonymisation Techniques – page 6 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[23] **Article 29 data protection working party** - Opinion 05/2014 on Anonymisation Techniques – page 11.

[24] **OECD** - Emerging Privacy Enhancing Technologies - Current Regulatory and Policy Approaches – 2023: *"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".*

[25] **ENISA** Report – Data Protection Engineering – 2022*: "The k-anonymity model […] is built on the idea that by combining sets of data with similar attributes, identifying information about any one of the individuals contributing to that data can be obscured. […] a dataset is considered to provide k-anonymity protection if the information for each data subject contained in the dataset cannot be distinguished from at least k-1 data subjects whose information also appears in the dataset. The key concept is to address the risk of re-identification of anonymized data through linkage to other available datasets."*

[26] **Article 29 data protection working party** - Opinion 05/2014 on Anonymisation Techniques – page 16: In contrast, a European working group has proposed the following definition: *"Aggregation and K-anonymity techniques aim to prevent a data subject from being singled out by grouping them with, at least, k other individuals. To achieve this, the attribute values are generalized to an extent such that each individual shares the same value. For example, by lowering the granularity of a location from a city to a country a higher number of data subjects are included. Individual dates of birth can be generalized into a range of*

How PETs relying on anonymization enhance privacy. As k-anonymity can ensure a complete anonymisation of personal data, **such technique provides very strong privacy safeguards**. The compliance with personal data protection requirements and restrictions is therefore limited to the collection and anonymization process and controller shall demonstrate the robustness of the k-anonymity technique implemented. K-anonymity also enables to fulfill **purpose limitation** and **integrity and confidentiality (security)**, when the anonymisation process is made immediately after personal data collection, (i) the data post-anonymization is no longer personal data, leading automatically to a limited risk of processing for non-compatible purpose and (ii) it limits drastically the risk of breach of any personal data.

Use case: The company IMMUTA has put in place k-anonymization techniques in relation with health data: "*Let's say you're looking at a data set of 100 individuals featuring basic identifying information — name, zip code, age, gender, etc. There is also information about each person's health status, which is what you want to study. Since health information must remain private according to data regulations like HIPAA,* ***k-anonymization could be used to generalize some identifying attributes and remove others entirely****. Information such as individuals' names is not relevant to health data in this case, so it can be removed.* ***Other data, such as zip code, can be broadened to a larger geographical area****. This removes the ability to connect specific health information to individuals with certainty, while still preserving the data's utility and effectiveness. In fact, k-anonymization for sensitive health data is one of its most common use cases."*[27]

Year	Gender	ZIP	Diagnosis
1957	M	750*	Heart attack
1957	M	750*	Cholesterol
1957	M	750*	Cholesterol
1964	M	750*	Heart attack
1964	M	750*	Heart attack

[28]

Practical insight: K-anonymity is a valuable technique in the field of online advertising since it prevents re-identification by anonymizing users data.

1.2.2. What is Differential Privacy and how does it impact privacy ?

General explanation. Differential privacy involves integrating perturbations (called "*noise*") into the database, mixing identification data with artificial data. By adding sufficient random noise to create aggregated data, this can prevent the identification of any individuals' data involved. Differential privacy allows to study larger statistical trends in a

dates, or grouped by month or year. Other numerical attributes (e.g. salaries, weight, height, or the dose of a medicine) can be generalized by interval values (e.g. salary €20,000 – €30,000). These methods may be used when the correlation of punctual values of attributes may create quasi-identifiers".

[27] **IMMUTA** – Everything you need to know about k-anonymity – 2021 - https://www.immuta.com/blog/k-anonymity-everything-you-need-to-know-2021-guide/

[28] **Article 29 data protection working party** - Opinion 05/2014 on Anonymisation Techniques – page 17.

dataset but protects data about individuals who participate in this dataset. The difficulty lies in balancing these disturbances with preserving the interest of the initial data[29][30].

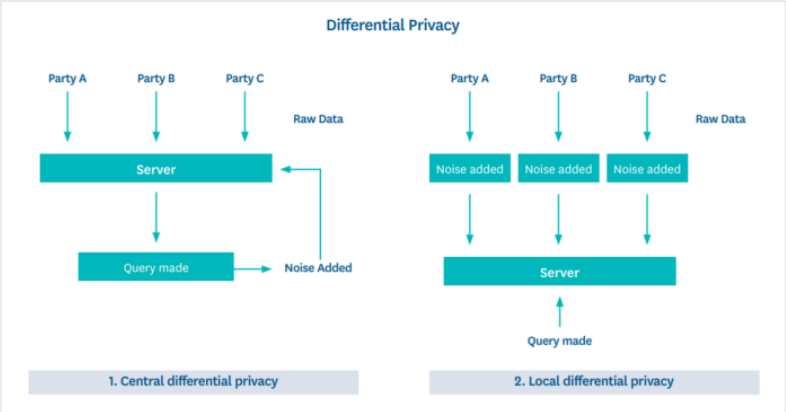


Figure 6: Differential Privacy
Source: CIPL

How PETs relying on anonymization enhance privacy. As differential privacy can ensure complete anonymization of personal data, **such technique provides strong privacy safeguards**, subject to demonstration of the robustness of the differential privacy technique implemented. The benefits of differential privacy in terms of privacy protection also relate to **purpose limitation** and **integrity and confidentiality (security)**, when the anonymization process is made immediately after personal data collection, (i) the data post-anonymization is no longer personal data, leading automatically to a limited risk of processing for non-compatible purpose and (ii) it limits drastically the risk of breach of any personal data.

Use case: Brave web browser has introduced new guarantees for its users based on differential privacy. It enables advertisers to get useful insights about the product feedback of a population without learning anything about the choices of individuals in the population. Brave describes this technology in three steps:

"1) the uncertainty of any particular user contributing any value;

2) blinding Brave to uncommon values through the secret-sharing mechanism (i.e., thresholding);

3) having some users contribute precisely defined amounts of dummy data to obscure the distribution of uncommon values." [31]

Practical insight: Differential privacy is considered a gold standard for rigorous privacy guarantees with two main variants: local and central differential privacy.

---

[29] **OECD** - Emerging Privacy Enhancing Technologies - Current Regulatory and Policy Approaches – 2023: *"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)".*

[30] **CIPL** – Privacy-Enhancing and Privacy Preserving Technologies: Understanding the role of PETS and PPTs in the Digital Age – December 2023: *"Differential privacy is a technical solution that uses a mathematical framework to safeguard privacy. By adding the right amount of random noise to analytical outputs from datasets, individual privacy is preserved while minimizing the trade-off on data accuracy. The purpose of differential privacy is to alter the data in a way that prevents the identification of any individuals' data involved. In differential privacy, the privacy loss parameter or privacy budget controls the amount of noise to be added. This parameter is measured in epsilon (ε) and regulates the trade-off between privacy and accuracy. Smaller values lead to greater privacy but lower accuracy. For example, ε=0 completely protects privacy at the cost of no accuracy as only noise is present. In this context, accuracy is defined as the proximity of the output from a differentially private dataset to the real output when analyzing the data".*

[31] **Brave** – Nebula: Brave's differentially private system for privacy-preserving analytics – September 2024 - *https://brave.com/blog/nebula/*

2. Data-masking and Privacy-preserving computation

2.1. What is Homomorphic Encryption (HE) and how does it impact privacy?

General explanations. Homomorphic encryption provides the ability to compute data while the data is encrypted. The result of such computation remains in encrypted form and can be read in clear only by the owner of the private key. As explained by ENISA, other PETs are regularly combined with homomorphic encryption[32][33].

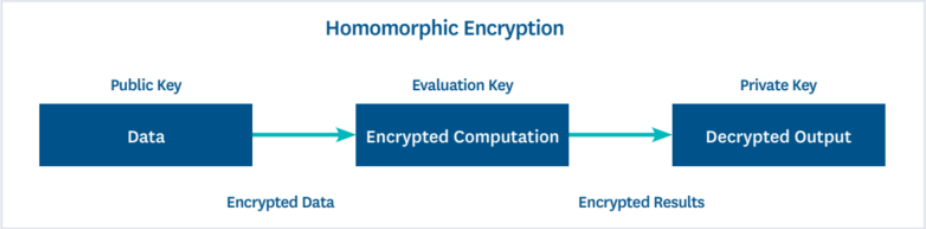


Figure 1: Homomorphic Encryption
Source: CIPL

To be noted, Microsoft recently developed an open-source homomorphic encryption technology in the form of a simple API enabling anyone, notably in the advertising sector, to use this complex technology[34].

How PETs relying on homomorphic encryption enhance privacy. The benefits of homomorphic encryption in terms of privacy protection relate in particular to the following principles:

- **Integrity and confidentiality (security)**, as homomorphic encryption allows data to remain encrypted while in use, and therefore hidden at all times, this allows to maintain strict confidentiality over the data and thus to reduce the security risks of data in use as well as the risk for data subjects in the event of data breach;
- **Purpose limitation**, by using homomorphic encryption, data remain encrypted throughout its processing, which minimizes the risk of use for incompatible purposes, **ensuring that the data is only accessible for specific and legitimate purposes**.

Use Case: The Institute of Electrical and Electronics Engineers gives a use case involving Microsoft's Election Guard: "*Today, homomorphic encryption can be used for more secure elections.*

[32] **ENISA** Report – Data Protection Engineering – 2022: *"Homomorphic encryption is a building block for many privacy enhancing technologies like secure multi-party computation, private data aggregation, pseudonymisation or federated machine learning to name a few. Homomorphic encryption allows computations on encrypted data to be performed, without having to decrypt them first. The typical use case for homomorphic encryption is when a data subject wants to outsource the processing of her personal data without revealing the personal data in plaintext".*

[33] **CIPL** – Privacy-Enhancing and Privacy Preserving Technologies: Understanding the role of PETS and PPTs in the Digital Age – December 2023 – page 25:*"Homomorphic encryption enables encrypted computations to be performed on data without first having to decrypt them. With non-homomorphic encryption schemes, data must be decrypted before any computations can be performed on it. This means that there is a period of time during which the data is vulnerable to interception or other attacks. By removing this opening, homomorphic encryption can help preserve the privacy and security of sensitive data".*

[34] **Microsoft SEAL** – Build end-to-end ecrypted data storage and computation services - https://www.microsoft.com/en-us/research/project/microsoft-seal/

Microsoft's Election Guard, for example, uses homomorphic encryption to ensure accurate voting results. ***Each vote is encrypted, and voters are given tracking codes (including the private key). Voters can then check if their vote was counted properly. At the same time, nobody else can see how that person voted.***[35]***"***

Practical insight: although homomorphic encryption is considered an outstanding technique, only a very small number of types of data processing can be encrypted, which prevents massive adoption. As of today, this technology does not appear to have been deployed in the online advertising sector.

2.2. What is Secure Multi-Party Computation (SMPC) and how does it impact privacy?

General explanation. Secure multiparty computation allows computation on data held across multiple parties without revealing or transferring any raw data, but only the results of the computation. Each party will perform computation on its data and the results are combined to obtain the final result without revealing any raw data. In order to produce an effective protocol, two cumulative conditions must be respected:

- Accuracy: the MPC protocol provides the correct output for the given function and input; and
- Confidentiality: no party should be able to learn anything other than the output of the MPC protocol[36][37].

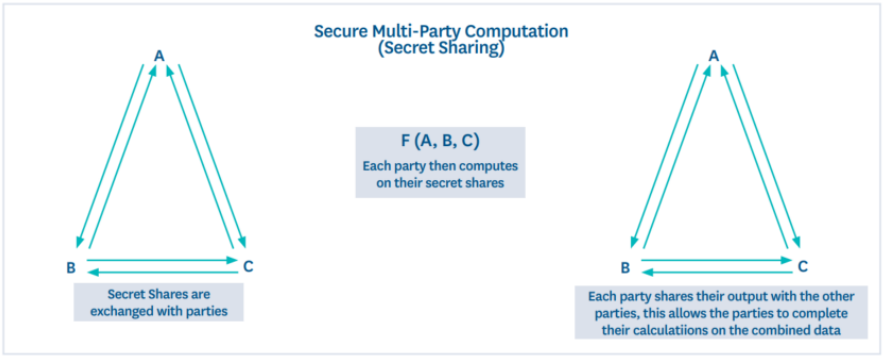


Figure 2: Secure Multi-Party Computation (Secret Sharing)
Source: CIPL

[35] **IEEE** – Homomorphic Encryption Use Cases - https://digitalprivacy.ieee.org/publications/topics/homomorphic-encryption-use-cases

[36] **ENISA** Report – Data Protection Engineering – 2022: *"The concept of secure multiparty computation (SMPC) refers to a family of cryptographic protocols that was introduced in 1986 and attempts to solve problems of mutual trust among a set of parties by distributing a computation across these parties where no individual party can see the other parties' data."*

[37] **CIPL** – Privacy-Enhancing and Privacy Preserving Technologies: Understanding the role of PETS and PPTs in the Digital Age – December 2023 – page 28: *"Secure multi-party computation provides a solution to allow multiple parties to compute on their combined data, without either party revealing any information about their input data. The objective is to protect the privacy of the parties while still enabling them to perform useful computations.*

Secure multi-party computation is implemented using a technique called "secret sharing." This technique is used to split each party's data (the secret) into different shares, which are then distributed among the other parties. The secret can only be reconstructed by combining a minimum number of shares. Each party then computes on their shares and may distribute their results to the other parties to help reach their target answer".

How PETs relying on secure multiparty computation enhance privacy. The benefits of secure multiparty computation in terms of privacy relate in particular to the following principles:

- **Integrity and confidentiality (security)**, as SMPC allows multiple parties to collaborate without revealing any raw data, the confidentiality of the data is assured. Moreover, regarding integrity, in event of a data breach involving one party, the data of the other parties remains protected, limiting the overall risk for the data subjects ;
- **Purpose limitation**, the fact that raw data is not shared between parties limits the risk of unauthorized data use and ensures that data is only accessible for specific and legitimate purposes;
- **Data minimization**, by enabling different parties to collaborate without sharing any information other than the final output, SMPC reduces the need to collect, store and duplicate the data.

It should be noted that the European Data Protection Board has issued recommendations in the context of international data transfers wherein it states that secure multi-party computation is an effective "*supplementary measure*" to ensure compliance with the level of protection required under EU law in a particular third country[38].

Use case: The World Wide Web Consortium (W3C) is currently developing a browser API for the measurement of advertising performance, known as the Privacy-Preserving Attribution API[39]. Its goal is to generate aggregate statistics about how advertising leads to conversions, without creating a risk to the privacy of individual web users. Within this technology, the aggregation and differential privacy implementation can be fully achieved using a Secure Multi-Party Computation system based on Prio and the Distributed Aggregation Protocol (DAP). This approach is the result of significant joint research efforts by contributors from Google, Meta and Mozilla.

Practical insight: In the same way as homomorphic encryption, SMPC has proven itself a very useful technique for some computations, and it is likely that even more computations can be done this way in the future. However, SMPC is a demanding technique, involving high investments in research effort.

2.3. What is Trusted Execution Environments (TEE) and how does it impact privacy?

General explanation. A trusted execution environment establishes a separation within the same computer processor in order to isolate some data considered as protected or sensitive from other less important data. Therefore, in the event of a breach or hacking on the untrusted part of the processor, the trusted part will not be necessarily damaged. The idea is that the part

[38] **EDPB** - Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - June 18, 2021 - https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

[39] **W3C - Privacy-Preserving Attribution: Level 1 - Editor's Draft, 6 March 2025- https://w3c.github.io/ppa/**

of the processor containing the protected data is isolated and is not intended to interact regularly with external environments, therefore limiting the risks of being damaged[40][41].

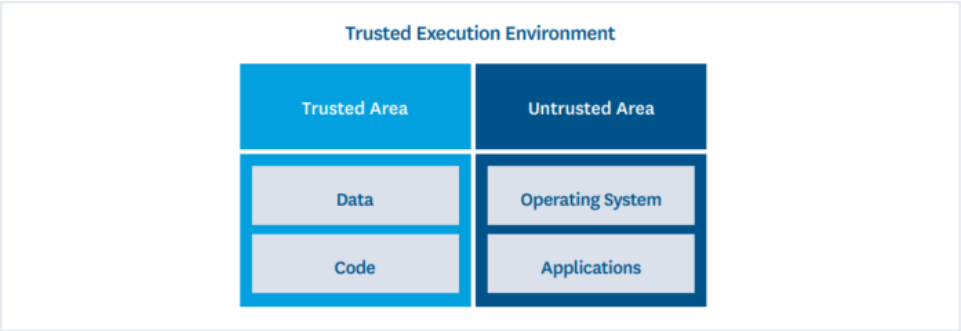


Figure 3: Trusted Execution Environment
Source: CIPL

TEEs and data clean rooms ("DCRs"). TEEs and DCRs are both technologies sharing the same goal, ie. enabling data processing in a secure and purpose-limited way. However, TEEs are mainly based on the notion of 'remote attestation' ensuring that the established rules are respected, whereas DCRs are based on an unverifiable statement. The degree of trust is where DCRs differ from TEEs, since trust shall be placed in the operator of the DCR to ensure privacy is maintained, when TEEs can be verified through attestations.

How PETs relying on TEEs enhance privacy. The benefits of TEEs in terms of privacy protection relate in particular to the following principles:

- **Integrity and confidentiality (security)**, by isolating user data within an independent and protected part of the processor, data integrity and confidentiality are necessarily increased. A TEE acts as a safeguard against data breach and limits the risk of unauthorized access to personal data ;
- **Purpose limitation**, by restricting the data only to permitted code, a TEE safeguards against others accessing and processing the data in unauthorized ways. Thus, a TEE requires data to be used only for the purpose clearly set out from the start.

Use Case: In 2024, Mozilla acquired Anonym, an adtech infrastructure focusing on improving privacy measures for data commonly shared between advertisers and ad networks. A key part of this process is where that data is sent and stored. Therefore, instead of advertisers and ad networks sharing personal user data with each other, increasing the risk to users every time a share is made, Mozilla encrypts it and sends it to a TEE. This technique still allows to unlock insights and value from data without enabling the development of cross-site behavioral profiles based on user-level data[42].

[40] **OECD** - Emerging Privacy Enhancing Technologies - Current Regulatory and Policy Approaches – 2023: *"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".*

[41] **CIPL** – Privacy-Enhancing and Privacy Preserving Technologies: Understanding the role of PETS and PPTs in the Digital Age – December 2023 – page 28: *"A trusted execution environment is a secure and isolated area within a computing system that provides a platform for running code and accessing data in a protected way. Applications running outside the trusted execution environment cannot access data within it, but applications running inside the trusted execution environment can access the data outside it".*

[42] **Mozilla Blog** – Using trusted execution environments for advertising use cases – December 3, 2024 - https://blog.mozilla.org/en/products/advertising/using-trusted-execution-envrionments-for-advertising-use-cases/

Practical insight: TEE can be used in a wide range of situations, and is technically less complicated to implement than SMPC. In the field of digital advertising, examples of implementation of this technique operate on server (not on device), keeping end-user data safe and inaccessible *per se* by third parties.

2.4. What is Private Information Retrieval and how does it impact privacy ?

General explanation. The concept of Private Information Retrieval (PIR) allows a user to extract data from a database without revealing to the database custodian (e.g. the database owner or administrator) which element has been searched for. To be relevant, a PIR protocol must provide two guarantees:

- Correctness: the information returned to the user must be correct;
- Privacy: the database must not learn anything from the user's queries, even if several queries are combined[43].

How PETs relying on private information retrieval enhance privacy. The benefits of private information retrieval in terms of privacy protection relate in particular to the following principles:

- **Data minimization**, by preventing the owner of a database from knowing the queries made by users, **PIR prevents the collection of additional, potentially personal data**;
- **Integrity and confidentiality (security)**, this system ensures greater integrity and confidentiality by preventing the database owner from collecting information about the user's queries. Since PIR involves the collection of less personal data, this may have a downward impact on the level of risk for the data subject in case of data breach.

Use Case: Chrome uses PIR technology as part of its system for detecting passwords compromised in data breaches, in order to preserve the integrity of its users' credentials[44]. In this process, Chrome first encrypts the user's credentials before transmitting the encrypted data to Google. The encrypted credentials are then compared against an encrypted database of known breached data. If a match is detected, Chrome issues a warning prompting the user to update their password. At no point does Google gain access to the user's actual usernames or passwords.

Practical insight: Private Information Retrieval is considered a valuable technology, but difficult to implement when the database is both very large and changing frequently. This makes it difficult to apply in online advertising, where the number of potential ads is extremely large and changes very frequently.

2.5. What is Synthetic Data and how does it impact privacy?

[43] **Cryptography Group of Stanford University** – Private Information Retrieval - https://crypto.stanford.edu/pir-library/: *"Private Information Retrieval (PIR) is a protocol that allows a client to retrieve an element of a database without the owner of that database being able to determine which element was selected. […] Additionally, Strong Private Information Retrieval (SPIR) is private information retrieval with the additional requirement that the client only learn about the elements he is querying for, and nothing else. This requirement captures the typical privacy needs of a database owner".*

[44] **Google Security Bloq - Better password protections in Chrome - How it works - December 10, 2019 - https://security.googleblog.com/2019/12/better-password-protections-in-chrome.html**

General explanation. The concept of synthetic data is to take an original data source and create new, artificial, dataset with similar statistical properties from it. The dataset can be fully synthetic or partially synthetic.

- fully synthetic data: in this case, all data are summarized, providing a stronger privacy than partially synthetic data. However, preserving dataset properties can be challenging;
- partially synthetic data: in this case, only the most sensitive data is summarized from a privacy perspective. The main advantage is that the general properties of the database are more easily preserved.

Synthetic data technique differs from the Differential Privacy technique: synthetic data is used to create artificial datasets without real data (at least without sensitive real data in the partially synthetic data hypothesis), whereas differential privacy involves processing real data into aggregates, and protects its confidentiality by adding noise[45][46].

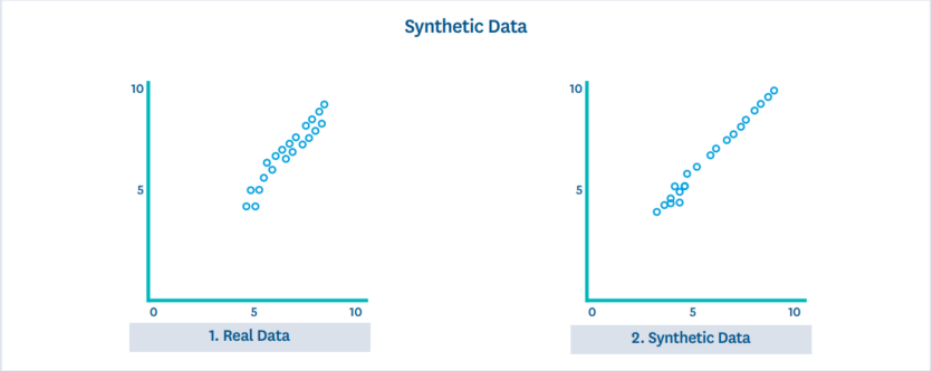


Figure 7: Synthetic Data
Source: CIPL

Replace real data with artificial data to safeguard privacy

How PETs relying on synthetic data enhance privacy. The benefits of synthetic data in terms of privacy protection relate in particular to the following principles:

- **Data minimization**, since the data processed is synthetic data, the processing of real data is limited. In short, the real data is processed only once, in order to synthesize it ;
- **Integrity and confidentiality (security)**, data confidentiality is ensured since data processed differs from real data. Also, the risk for personal data to be access without authorization is reduced ;
- **Purpose limitation**, in the same way, as real data is not used, synthetic data technique safeguards against accessing or processing the real data in unauthorized ways.

Use Case: A well-known use case involves the learning of Alexa developed by Amazon. To the challenge of how to bootstrap the machine learning models that interpret customer requests,

[45] **EDPS** – Synthetic Data - https://www.edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en: *"Synthetic data is artificial data that is generated from original data and a model that is trained to reproduce the characteristics and structure of the original data. This means that synthetic data and original data should deliver very similar results when undergoing the same statistical analysis".*

[46] **CIPL** – Privacy-Enhancing and Privacy Preserving Technologies: Understanding the role of PETS and PPTs in the Digital Age – December 2023 – page 41: *"Synthetic data refers to artificially generated data that resembles real data. Personal information may be replaced with fake data, or all original data may be removed. By carefully generating synthetic data, an alternative to real data can be provided that protects privacy, without losing the value from data. It can be used for various purposes, including data analysis, machine learning model training, testing and data sharing without the risk of exposing sensitive information. There are two broad types of synthetic data: fully synthetic and partially synthetic".*

without the ability to learn from customers interactions, the solution used a synthetic data technique.[47]

Practical insight: As of the publication date of this white paper, it appears that while synthetic data is a valuable technique, it is challenging to implement beyond the realms of analysis and research, including in the field of digital advertising.

[47] **Amazon** - Tools for generating synthetic data helped bootstrap Alexa's new-language releases : https://www.amazon.science/blog/tools-for-generating-synthetic-data-helped-bootstrap-alexas-new-language-releases

3. Access, communication and storage

According to the ENISA taxonomy, this category includes the following sub-categories: communication channels (**3.1.**), privacy preserving storage (**3.2.**), privacy-enhancing access control, authorization and authentication (**3.3.**).

3.1. Communication channels

In the context of data protection engineering, communication channels should not only focus on their primary security function but also integrate additional privacy-enhancing features. Among these technologies, ENISA identifies end-to-end encryption (3.1.1) and proxy routing (3.1.2).

3.1.1. What is End-to-End Encryption (E2EE) and how does it impact privacy?

General explanation. E2EE is a method of encrypting data that can only be decrypted by authorized parties. The special feature of end-to-end encryption is that the data is encrypted as soon as it is sent and then decrypted as soon as it is received by the authorized terminal, which is the only one to hold the decryption key. Anyone else catching the message would only be able to read an encrypted message.

It should also be noted that E2EE differs from homomorphic encryption:

- E2EE is a method which ensures that data can only be decrypted on the authorized terminal.
- Homomorphic encryption is a method which ensures that only the results of operations on encrypted data can be decrypted (the data itself remains encrypted) [48][49].

How PETs relying on E2EE enhance privacy. The benefits of E2EE in terms of privacy protection relate in particular to the following:

- **Integrity and confidentiality (security),** E2EE ensures that encrypted data can only be decrypted in the authorized terminal. Therefore, this protects data from unauthorized access during transmission, guaranteeing its security and limiting the risk for data subject in case of data breach ;
- **Purpose limitation,** as the data is encrypted, only the sender and the recipient can decrypt and process it. This protects data from unauthorized access and therefore from unauthorized use of the data.

[48] **IBM** – What is E2EE ? - https://www.ibm.com/topics/end-to-end-encryption: *"Data encryption is the process of using an algorithm that transforms standard text characters into an unreadable format. To explain, this process uses encryption keys to scramble data so that only authorized users can read it. End-to-end encryption uses this same process, too. However, it takes it a step farther by securing communications from one endpoint to another".*

[49] **ENISA** Report – Data Protection Engineering – 2022 – page 19: *"End-to-End Encryption (E2EE) is a method of encrypting data and keeping them encrypted at all times between two or more communicating parties. Only the parties involved in the communication have access to the decryption keys".*

Use Case: PAIR (Publisher Advertiser Identity Reconciliation) protocol[50] is a privacy-centric approach to enable advertisers and publishers to reconcile their first-party data for advertising use cases without the reliance on third-party cookies. The advertiser and the publisher first-party data is each encrypted three times with three different encryption keys: an advertiser key, a publisher key, and a private shared key between the advertiser and publisher. These keys are unique for every advertiser-publisher relationship. Each participating entity has access to up to two of the keys, ensuring that no single party can access all three keys simultaneously to decrypt the data back to the original raw data.

Practical insight: end-to-end encryption is easily available and provides a very high guarantee of security and integrity. Therefore, it is strongly recommended to implement this technology, including in the digital advertising sector.

3.1.2. What are Proxy & Onion routing and how does it impact privacy?

General explanation. Basically, a proxy is a server that acts as an intermediary between a request and a response, thereby increasing the complexity of tracking down the user.

In onion routing (more complex technique), data is initially wrapped in multiple layers of encryption at the entry node. As it travels through various intermediate nodes, each one removes a layer of encryption, uncovering the next destination. This process continues until the data reaches the final exit node. This means that each relay knows neither the content of the data nor the final recipient[51].

How PETs relying on proxy & onion routing enhance privacy. The benefits of "*Proxy & Onion routing*" in terms of privacy protection relate in particular to the following principles:

- **Integrity and confidentiality (security),** the use of "*Proxy & Onion routing*" ensures a high level of security, ensuring data integrity and confidentiality by increasing the complexity of the process of communicating data from one terminal to another;
- **Data minimization**, these techniques ensure that the server never acquires the IP address from which the web page was requested, leading to data minimization improvements;
- **Purpose limitation, "***Proxy & Onion*" routing does not alter the content of data or the purposes for which it is processed. Its sole role is to guarantee the anonymity of the data path, which means that data is used solely for the purposes for which it was collected, without alteration or misappropriation by third parties.

Use Case: Tor is a well-known use case:

- User's internet service provider, and anyone watching their connection locally, **will not be able to track their internet activity, including the names and addresses of the websites visited.**
- **The operators of the websites and services that the user uses, and anyone watching them, will see a connection coming from the Tor network instead of**

[50] **IAB Tech Lab - Publisher Advertiser Identity Reconciliation (PAIR) - January 21, 2025 - https://iabtechlab.com/PAIR/**

[51] **ENISA** Report – Data Protection Engineering – 2022: *"In onion routing user traffic is routed through a series of relay servers and each relay server receives layered encrypted data without knowing neither the original sender nor the final recipient".*

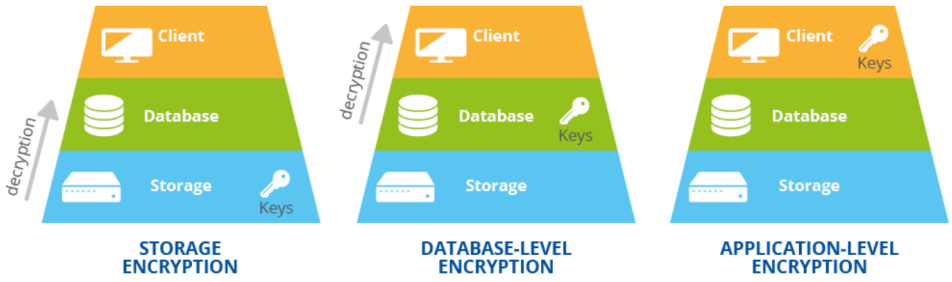
user's real Internet (IP) address, and will not know who user is unless they explicitly identify.[52]

Practical insight: These techniques tend to be implemented across sectors and are likely to be increasingly important in the future. In digital advertising, concealing the IP address from advertisers' servers is a useful privacy measure. As a result, Proxy and Onion routing are important to ongoing discussions within the browser community.

3.2. What is Privacy Preserving Storage and how does it impact privacy?

General explanation. The Privacy-Preserving Storage refers to a data management technique designed to protect the confidentiality of stored data, while enabling its use. As specified by ENISA, encryption is the main technique used and it can apply at different levels (storage, database or application) [53].

Figure 2: Database Encryption Options



How PETs relying on Privacy-Preserving Storage enhance privacy. The benefits of Privacy Preserving Storage in terms of privacy protection relate in particular to the following principles:

- **Integrity and confidentiality (security),** the very purpose of "*Privacy Preserving Storage*" is to ensure the confidentiality of data, notably through the use of cryptography;
- **Purpose limitation**, as the data is encrypted at various storage levels, Privacy-Preserving Storage protects data from unauthorized access and therefore from unauthorized use of the data.

Use Case: A concrete example of this principle is provided by WhatsApp, to ensure privacy for user contacts registered on the application, contact names are first encrypted using a symmetric encryption key generated by the user's device, and then stored in the HSM-based Key Vault (hardware security model). Then, the storage and retrieval of the contact encryption key occurs via an end-to-end encrypted channel between the client and the hardware security model, ensuring that the data in transit remains opaque to WhatsApp[54].

[52] **TOR** – About TOR Browser - https://tb-manual.torproject.org/about/

[53] **ENISA** Report – Data Protection Engineering – 2022: *"Privacy preserving storage has two goals: protecting the confidentiality of personal data at rest and informing data controllers in case a breach occurs. Encryption is the main technique used to protect the data confidentiality from unauthorized access. Depending on the constraints of data controllers, it can be applied at three different levels: (i) storage-level, (ii) database level and (iii) application-level encryption".*

[54] **Meta** - IPLS: Privacy-preserving storage for your WhatsApp contacts – October 2024 - https://engineering.fb.com/2024/10/22/security/ipls-privacy-preserving-storage-for-your-whatsapp-contacts/

Practical insight: Privacy-Preserving Storage are likely to be increasingly implemented in the future, includingin the digital advertising sector.

3.3. Privacy-enhancing access control, authorization and authentication

This subcategory includes the following techniques: Attribute Based Credentials (**3.3.1**) and Zero-Knowledge Proofs (**3.3.2**).

3.3.1. What is Privacy-Enhancing Attribute Based Credentials and how does it impact privacy?

General explanation. Attribute-Based Credentials (ABC) is a cryptographic system in which a user receives credentials (certificates) containing personal attributes (such as age, employment status or citizenship). These credentials enable the user to prove that he possesses certain attributes (for example age over 18) without revealing the specific details of these attributes (for example the specific age) when authenticating or accessing services. This Attribute-Based Credentials requires the intervention of a third party to authenticate the veracity of the attribute and therefore deliver the credential[55].

How PETs relying on Attribute Based Credentials enhance privacy. The benefits of Attribute Based Credentials in terms of privacy protection relate in particular to the following principles:

- **Data minimization**, as the personal data corresponding to the attributes are maintained only by the third party and not with all the providers of services to which the data subject wishes to have access, ABC can be seen as a factor improving data minimization;
- **Integrity and confidentiality (security**), by going through a trusted third party, users only have to communicate the proof of their data, which greatly increases confidentiality: the personal data corresponding to the attributes are maintained only by one trusted third party and not shared with all the providers of services to which the data subject wishes to have access;
- **Purpose limitation**, as the objective of "*Attribute Based Credentials*" is to be able to authenticate or prove a characteristic by communicating the credential delivered by a third party while not communicating the exact data, data is protected from unauthorized use.

Use Case: *"Attribute-based credential systems, especially when implemented on smart cards, can be used both offline and online. An example of an offline use case is the use of a tobacco vending machine. To prevent the sale of tobacco to minors, the vending machine can use ABC technology to verify that the buyer is over 18 (or whatever the appropriate legal limit is).* ***For this to work, users must be able to obtain a credential from the municipality that contains an « over 18 » attribute****. When buying cigarettes the user inserts her smart card in the vending machine and proves she is over eighteen and from there on continues the purchase transaction.[56]"*

[55] **ENISA** Report – Data Protection Engineering - 2022: *"Attribute Based Credentials (ABC) allow the authentication of an entity by selectively authenticating different attributes without revealing additional information that are typically used and could very well include personal data".*

[56] The ABC of ABC: An analysis of Attributed-Based Credentials in the light of Data Protection, Privacy and Identity - https://www.cs.ru.nl/J.H.Hoepman/publications/abc-of-abcs.pdf - page 3.

Practical insight: Attribute-Based Credentials and zero-knowledge proofs are highly effective and should be used in combination. Specifically, in the online advertising sector, these techniques utilize a token system to prove that an advertisement led to a conversion, without disclosing any additional information about the user or the conversion itself.

3.3.2. What is Zero-knowledge Proof and how does it impact privacy?

General explanation. Zero-Knowledge Proof is a cryptographic protocol that allows one party (the prover) to prove to another party (the verifier) that a certain assertion is true, without revealing any information about that assertion, other than the fact that it is true.

Zero-knowledge proof differs from attribute-based credentials in that no information is revealed, even to a third party, other than the truth of the claim[57][58].

How PETs relying on Zero-knowledge proof enhance privacy. The benefits of Zero-knowledge proof in terms of privacy protection can be summarized as follows: as the objective of "Zero-Knowledge Proof" is to be able to authenticate or prove a characteristic by communicating only the proof of the claim, this technique allows to prove the validity of a claim without revealing any additional information which is in line with the principles of **Data minimization**, **Integrity and confidentiality (security**) and **Purpose limitation**.

Use case. The World Wide Web Consortium (W3C) is currently developing a browser API for the measurement of advertising performance, known as the Privacy-Preserving Attribution API[59]. As mentioned above, within this technology, the aggregation and differential privacy implementation can be fully achieved using a Secure Multi-Party Computation system based on Prio and the Distributed Aggregation Protocol (DAP). The API uses zero-knowledge proofs within its multi-party computation framework as an anti-abuse mechanism: it allows verifying that each browser contributes only the permitted amount to the aggregate.

Practical insight: Attribute-Based Credentials and zero-knowledge proofs are highly effective and should be used in combination. Specifically, in the digital advertising sector, these techniques utilize a token system to prove that an advertisement led to a conversion, without disclosing any additional information about the user or the conversion itself.

---

[57] **Forbes** – What are zero-knowledge proofs? - https://www.forbes.com/sites/forbestechcouncil/2023/02/07/what-are-zero-knowledge-proofs/: *"zero-knowledge proof" as follows: "In a ZKP, two parties are involved: the prover and the verifier. The prover aims to establish a claim, and the verifier is accountable for verifying the claim. The prover can demonstrate to the verifier that a statement is accurate without revealing any supplementary information regarding the statement. This is done by providing proof, or a small amount of information, that can be verified by the verifier to ensure that the statement is true".*

[58] **CIPL** – Privacy-Enhancing and Privacy Preserving Technologies: Understanding the role of PETS and PPTs in the Digital Age – December 2023 – page 32: *"Zero-knowledge proof is a technique that enables one party (the prover) to prove a claim to another party (the verifier) without revealing anything more than the truth of the claim. Through the use of complex mathematical algorithms, the proof is generated in such a way that it is computationally infeasible for someone who does not know the claim to generate a similar or related proof.*

A zero-knowledge proof has three main properties:

- *Completeness: If the claim being proved is true, then an honest verifier will be convinced of this fact with high probability.*
- *Soundness: If the prover does not know the claim, then he cannot deceive the verifier with high probability.*
- *Zero-knowledge: The verifier does not learn anything other than the validity of the claim".*

[59] **W3C - Privacy-Preserving Attribution: Level 1 - Editor's Draft, 6 March 2025- https://w3c.github.io/ppa/**

4. Transparency, Intervenability and User Control Tools

General explanation. Transparency, intervenability and user control tools cover all the instruments put in place to ensure that individuals have access to information and can intervene in the processing of their data. The idea behind this category is that no matter what confidentiality and personal data protection measures are in place, they only make sense if users are able to understand and exercise their rights[60].

How PETs relying on transparency, intervenability and user control tools enhance privacy. The benefits of transparency, intervenability and user control tools in terms of privacy protection relate in particular to the following principles:

- **Transparency** is the very purpose of this category of measures, through the drafting of privacy policies, consent management processes, etc. Anything that enables users to be informed about how their data is being processed;
- **End-user empowerment**, some instruments are designed to give users control over how their data is processed. These tools enable users to be able to better control and choose the way their data are processed, and therefore better enforce their rights. If the data subject controls strictly the use of its personal data, it constitutes the essence of privacy by design. In consequence, it impacts positively all other privacy principles.

Use Case: A multitude of methods and tools aim at increasing the level of information and control of end-users, including privacy policies, consent management systems, exercising right of access, right to erasure, right to rectification, etc. [61]

* * *

[60] **ENISA** Report – Data Protection Engineering – 2022: *"A key element in any data protection concept is the enablement of human individuals to exercise their data protection rights themselves. This involves both access to information on data processing (transparency) and the ability to influence processing of their personal information within the realm of a data controller or data processor (intervenability). In this respect, a multitude of approaches and topics emerged from the privacy research community that can help implementing these rights and correlated services at data processing institutions".*

[61] Ibid.


THE GOOD
ADVERTISING
PROJECT