The marketers' perspective on unlocking Privacy Enhancing Technologies (PETs) in personalised marketing and advertising communications

Executive summary

1. Introduction: Context and objectives 2

a) The value of digital marketing for consumers and businesses 2

b) The increasing demand for privacy and safety as key drivers of public trust in personalised marketing and advertising practices 3

c) Purpose of the paper 3

2. What are Privacy Enhancing Technologies (PETs)? 4

2.1. Definition 4

2.2 PET use cases in data-driven marketing and personalised advertising 6

2.3 Insights from FEDMA's member survey 8

3. Benefits of PETs for businesses and consumers 10

3.1. Businesses' benefits 10

3.2. Consumers' benefits 12

4. Barriers to the broader adoption of PETs 14

4.1 Regulatory and legal barriers 14

4.2 Informational and operational barriers 16

4.3 Economic and market barriers 16

5. Policy recommendations for supporting the development and adoption of PETs 18

5.1 Recommendations for Industry 18

5.2 Recommendations for Policymakers 20

6. Conclusion - Unlocking the potential of PETs in marketing and advertising 23

1. Introduction: Context and objectives

a) The value of digital marketing for consumers and businesses

Digital marketing provides substantial benefits directly to European consumers. The average European consumer receives an estimated €212[1] worth of free online services per month, including essential tools like news, email and search engines, all of which are largely sustained by digital advertising. In parallel, 80% of consumers find online ads useful and prefer fewer, more relevant ads over generic, mass-distributed ones[2]. When consumers encounter a helpful ad, over 70% describe it as a positive experience. Digital advertising also empowers consumers by providing convenient access to a wide array of products and services, facilitating price comparisons, and offering access to valuable information like product reviews, which significantly reduces uncertainty and boosts confidence in purchasing decisions. This enhanced access to information and personalised recommendations ultimately leads to more informed choices and a more tailored, efficient shopping experience for individuals across the EU.

In parallel, digital marketing is a vital engine for economic growth and societal impact across the European Union. According to a recent study[3], by enabling businesses to connect with customers more precisely, digital advertising is currently generating €100 billion in additional sales for EU businesses, contributing €25 billion to our GDP and supporting nearly 600,000 jobs. This is particularly beneficial for small and medium-sized businesses (SMBs), with 86% reporting increased revenue and 80% attracting more customers through personalised digital advertising. It also empowers SMBs to expand into new markets, with 34% leveraging digital advertising to reach new regions. Beyond digital advertising, other digital marketing channels demonstrate high returns on investment (ROI) for businesses. 30% of global marketers consistently rate email marketing as having the highest ROI among digital channels while another 43% rated it as having medium ROI. This highlights the diverse ways digital tools contribute to commercial success.

The value of digital marketing extends beyond the commercial sector. Non-governmental organisations (NGOs) are increasingly using digital marketing to educate and connect with people and donors while creating significant positive societal impact. For example, Save the Children Germany's digital campaign in 2024 raised over €750,000 and gained 4,500 new supporters, while WWF Spain's 2023 online campaign led to a 4.5-point increase in behavioural impact, mobilizing 91,600 people to adopt eco-friendly habits[4]. These examples demonstrate that digital marketing is a powerful tool for both economic prosperity and critical social change.

[1] IAB Europe, Kantar Media, Optimisation Over Reform - Understanding EU consumers' perception and knowledge of the ad-funded internet and related privacy rights issues, April 2025

[2] Centre for Information Policy Leadership (CIPL) & Public First, The Impact of Digital Advertising on Europe's Competitiveness: A Study on the Role of Digital Advertising in Europe, March 2025

[3] Implement Consulting Group, Personal Touch, A €100 billion boost to EU competitiveness from personalised ads, May 2025

[4] ThinkYoung, Digital Ads: Creating the Right Ad Tech Ecosystem for Privacy-Friendly Innovation and Growth in Europe, April 2025

b) The increasing demand for privacy and safety as key drivers of public trust in personalised marketing and advertising practices

In recent years, the increasing demand for privacy and safety has become a defining factor in shaping consumer expectations and trust in personalised marketing and advertising. While consumers clearly recognize the benefits of personalised approaches, such as seeing more relevant products, receiving valuable discounts, and even supporting the existence of "free" online services, a significant and persistent concern about data misuse remains. As individuals grow more aware of how their data is collected and used online, they are placing greater value on transparency, control, and data protection as drivers of the trust that they place in an organisation.

Indeed, according to the GDMA 2022 Consumer Attitudes to Privacy Study[5], for 39% of consumers across surveyed markets, trust ranks among the top three factors influencing data sharing, outperforming even the prospect of receiving free products or services. Crucially, transparency remains a cornerstone of building this trust: a significant 77% of global consumers emphasize the importance of clarity around how their data is collected and used when they consider sharing personal information. This shift is particularly evident in the European regulatory context, where frameworks like the GDPR have elevated privacy from a compliance requirement to a core element of responsible business practices.

While consumers increasingly take responsibility for their own data security, there is a growing expectation for the industry to uphold high standards of privacy and offer robust control mechanisms. In this environment, companies that prioritize privacy and user-centric data strategies are better positioned to earn and retain consumer trust. Ultimately, trust in personalised marketing today hinges not just on relevance and value, but increasingly on how securely and ethically personal data is handled.

c) Purpose of the paper

To that end, this paper aims to provide an overview of the main privacy-enhancing technologies (PETs) currently utilised by marketers, shedding light on the substantial benefits PETs can offer for both consumers and businesses, but also the current challenges hindering a faster and broader uptake of these crucial technologies. The analysis is informed not only by ongoing policy and technical discussions but also by the results of an internal survey conducted by FEDMA among its members to better understand how marketers are currently approaching PETs. As PETs have the potential to improve on data protection outcomes and better align with consumer expectations for privacy, transparency and safety, while unlocking and sustaining the benefits of digital marketing, it is imperative for both the industry and policymakers to collaboratively support the investment, development, and widespread adoption of PETs. By embracing solutions that allow for data utility while minimizing personal data exposure, we can cultivate an ecosystem where personalised experiences are delivered securely and ethically, ultimately strengthening consumer trust and ensuring a sustainable and responsible future for the digital economy in the EU.

[5] *GDMA, Global Data Privacy, What the Consumer Really Thinks, Foresight Factory*, 2022

2. What are Privacy Enhancing Technologies (PETs)?

Privacy-Enhancing-Technologies (PETs) is an umbrella term to designate multiple tools, technologies and techniques used to improve security, maintain user privacy, through an additional layer of protection, for instance, by minimizing the amount of data processed by third parties.

2.1. Definition

- Explanation of PETs are a broad suite of engineering techniques that can safeguard and enhance privacy and security by minimizing the collection, use, retention, and exposure of data with technical assurance/verification while enabling insights from data that power products and services.
  We can group PET technologies into two broad themes:
    - Those that add isolation protection, and
    - Those that anonymize data to make it safer for processing and exploration.

  When used effectively, PETs can provide meaningful technical privacy and data protections in a broad range of applications.
- Overview of key PET categories, including (but not limited to):
    - **Differential Privacy**[6]: Differential Privacy makes small changes (sometimes referred to as adding 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).
    - **Federated Learning**[7]: Federated learning (FL) is a privacy-enhancing technology that enables machine learning (ML) models to be trained without the need for centralised data collection. Instead of collecting raw data in a central location, federated learning keeps the data at its source, such as on user devices or within data silos and then the ML model will be trained there.
    - **Homomorphic encryption (HE)**[8]: 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.

[6] Ibidem
[7] Google Research Blog, Federated Learning: Collaborative Machine Learning without Centralised Training Data, April 2017
[8] Ibidem

- **Pseudonymisation**[9]: Pseudonymisation 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. Most recently, in Europe, the EUCJ has reasserted the relative nature of anonymity (see EDPS v SRB C-413/23P). The case confirmed that pseudonymised data held by a processor without reasonable means to reidentify the dataset (i.e. the key remains with the controller) should not be considered personal data. It is expected that further clarification on anonymity will arise shortly from regulatory bodies in the near future. The relative approach to anonymity has already been reflected in the Digital Omnibus proposal through the amendment of the definition of personal data, as well as a mandate for an implementing act to specify criteria for determining when data resulting from pseudonymisation is no longer considered personal data.[10]
- **Anonymisation**[11]**:** 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. Once data is truly anonymous and individuals are no longer identifiable, the data will not fall within the scope of the GDPR. However, there remains uncertainty for what counts as anonymised due to different standards for the acceptable degree of identifiability, and strict regulatory interpretations, making it extremely challenging to achieve anonymisation.
- **Secure Multi-Party Computation (MPC)**[12]: 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 Homomorphic encryption **(**HE) can be used to aggregate and compute data from multiple parties. Like FL, MPC remains unused among respondents with only a few actors in the ecosystem starting exploring use cases for marketing (e.g. Snowflake, Infosum, Habu, Google and Meta).

[9] OECD, *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches*, OECD Digital Economy Papers No. 351 (March 2023)

[10] Proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), Arts. 4 and 41a.

[11] Ibidem

[12] OECD, *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches*, OECD Digital Economy Papers No. 351 (March 2023)

- **Trusted Execution Environments (TEEs)**[13]: A trusted execution environment (TEE) is a dedicated area on a computer processor that is separated and secured from the operating system. It can process 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. Adoption remains niche (12%) but is growing quickly.

2.2 PET use cases in data-driven marketing and personalised advertising

- Use case 1: Targeting and Data Matching
  - For years, digital advertising has relied on third-party cookies and other identifiers to deliver relevant ads to consumers. This technology, while effective, created significant user privacy challenges, leading the industry to invest into innovative solutions that allow brands to reach their customers while respecting their privacy. PETs play an important role here because they can be used to build ads products that balance privacy and commercial utility. The central challenge for advertisers and publishers today is how to continue leveraging their valuable first-party data—such as customer email lists or purchase histories—for effective ad campaign targeting while also striking the balance between the need for customer privacy and innovation. Sharing raw customer data with advertising platforms is a non-starter from both a privacy and a business confidentiality perspective. This is the critical opportunity that Privacy-Enhancing Technologies (PETs) are now being deployed to solve. To address this challenge, new solutions are emerging that fundamentally reshape how advertiser and platform data can interact. One of the most promising applications is in the area of audience matching, exemplified by Google's Confidential Matching. It uses Private Set Intersection (PSI) and Trusted Execution Environments (TEEs) to allow advertisers to match their customer lists against platform data securely. Data is encrypted locally by the advertiser, and the matching process is isolated so neither party can see the other's raw data. This enables the output to be used for effective ad targeting based on aggregate results, creating a sustainable, privacy-safe standard for the future of advertising.
- Use case 2: Measuring ad effectiveness
  - PETs are also revolutionizing ad measurement, allowing advertisers to gauge campaign effectiveness without user-level tracking. Privacy-Preserving Attribution (PPA), pioneered by Mozilla, addresses this. To accomplish this,

[13] Ibidem

Mozilla's proposal utilizes advanced cryptographic protocols, primarily Multi-Party Computation (MPC) and secret sharing. This system splits attribution data into encrypted pieces, which are processed by multiple, non-colluding servers. No single party can see an individual's data, only the final, aggregated conversion numbers. This allows advertisers to see which ads lead to conversions, like purchases or sign-ups, without following users across the web.
When a user clicks an ad and later converts, the browser sends these anonymised data shares to be securely tallied, providing valuable, aggregated measurement insights while keeping individual Browse history completely private.

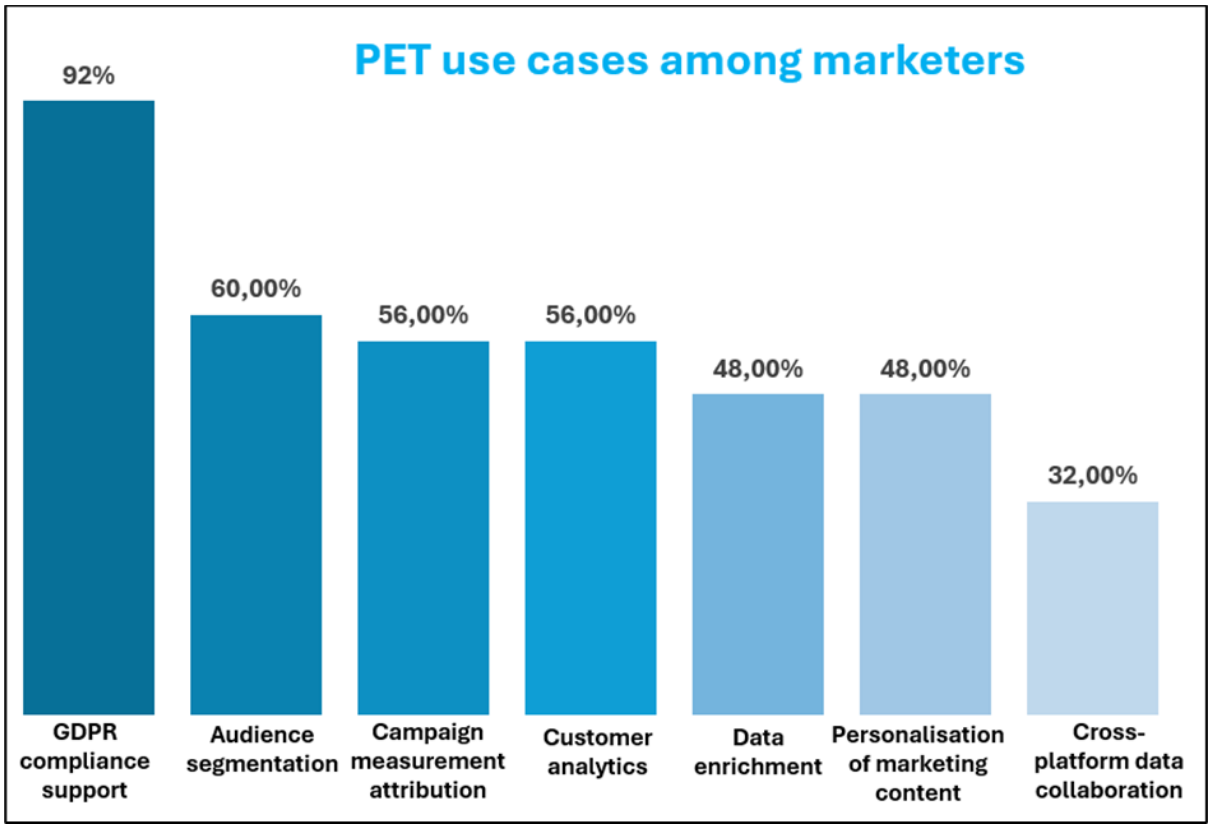
- Use case 3: Security
    - Secure Multi-Party Computation (SMPC) for ad campaign measurement. SMPC allows multiple parties to collaborate on data analysis without revealing their individual, private data to one another. In advertising, this can address security concerns around data sharing and privacy. Using SMPC, the advertiser and publisher can jointly compute the aggregated results, like how many users saw the ad and made a purchase, without either party revealing their raw customer data.

    - Differential privacy (DP) is a technique that adds a controlled amount of statistical "noise" to a dataset, making it virtually impossible to identify individual users while maintaining the overall statistical properties of the data. This can be used to combat ad fraud. A company can apply DP when querying aggregated ad impression data to measure the unique reach of a campaign across devices. The added noise prevents bad actors from reverse-engineering individual user data from the query results. DP can also be used with federated learning to detect click fraud by integrating web-based ad interaction data with retail point-of-sale metrics.

    - The Swiss Federal Department of Defence, Civil Protection and Sport (DDPS) and major financial institutions (Swiss National Bank, SIX, and Zurich Cantonal Bank) demonstrated the power of Privacy-Enhancing Technologies (PETs) to enhance national cyber resilience. The initiative leveraged Confidential Computing and secure Data Clean Rooms from Decentriq to identify and analyse common email phishing threats across organisational boundaries. This collaboration model allowed participants to share insights, detect new campaigns, and compare defence postures without directly exposing sensitive, unencrypted data to any party. The project proved the technical feasibility of using a neutral, protected environment to derive actionable threat intelligence, supporting the goals of the National Cyberstrategy by securely bridging the private and public sectors.

2.3 Insights from FEDMA's member survey

This survey was conducted by FEDMA between June and August 2025. It was designed to collect insights into the adoption and application of Privacy Enhancing Technologies (PETs) within data-driven marketing practices. The objective is to support FEDMA in understanding current industry approaches, identifying key challenges, and assessing the types of support needed to foster privacy-preserving innovation. Participants were FEDMA members and partners, representing key players in the data-driven marketing industry in Europe. Approximately 50 participants were invited to share their experiences and perspectives on PETs, including implementation strategies, perceived benefits, and barriers to adoption. All responses were treated as confidential and analysed to ensure anonymity.



Question: *For which use cases are you applying PETs? (Select all that apply)*

Uptake of PETs by European data-driven marketers

Anonymisation and pseudonymisation seem to be the most frequently used technique among respondents with a 76% adoption rate. The widespread adoption likely reflects its explicit recognition under existing legislation (e.g. GDPR, Data Act), corroborating the survey's insight that legal compliance support is the most common PET use case (92%).

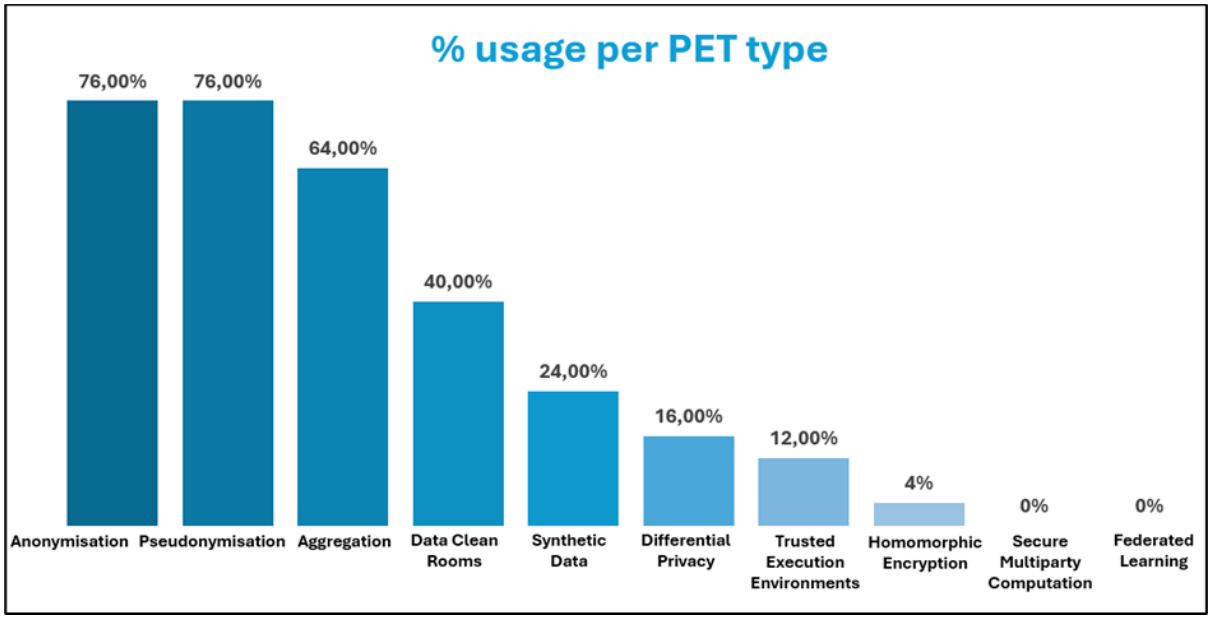
Aggregation is also commonly used (64%), referring to the process of consolidating and summarizing large amounts of raw data into a more digestible format. Once the aggregation process is complete, the data is placed in a central repository like a data

warehouse where team members can easily access and use it for analysis, marketing campaigns, and decision-making[14].

Data clean rooms (40%) are designed to be a secure, neutral, and protected environment where multiple parties can unify and jointly analyze their data. In short, user level data is sent into a data clean room by numerous parties, it gets aggregated in the secure space, and the resulting data is fed back out as a cohort.[15]

Synthetic data (24%) 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. The degree to which synthetic data is an accurate proxy for the original data is a measure of the utility of the method and the model[16].

Differential privacy is used by only 16% of respondents (see table below), its technical and implementation complexity may limit wider adoption.



Question: Which PETs is your organisation currently using? (Select all that apply)

[14] Source: Twilio : https://www.twilio.com/en-us/resource-center/data-aggregation
[15] Source: Adjust: https://www.adjust.com/glossary/data-clean-room/
[16] Source: European Data Protection Supervisor: https://www.edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en#:~:text=Tech%20Champion:%20Robert%20Riemann,in%20comparison%20to%20real%20images.

3. Benefits of PETs for businesses and consumers

3.1. Businesses' benefits

a) Accelerating commercial growth through safe data innovation

PETs are redefining how companies safely and responsibly unlock the power of data. By embedding privacy into the way data is analysed and shared, businesses gain access to new commercial opportunities without increasing regulatory risk.

- Unlock new revenue streams and access high-value data through secure collaboration
  PETs allow organisations to extract actionable insights from sensitive data without exposing raw personal information. By enabling secure, privacy-compliant data collaboration, using tools such as secure multi-party computation[17]or Trusted Execution Environments, businesses can confidently engage in joint analytics with partners, platforms, and public sector entities. This is also corroborated by FEDMA's internal survey, with 28% of respondents saying that PETs enabled them to launch new partnerships and collaborations (see table below). The use of PETs can also facilitate access to high-value datasets that were previously inaccessible due to legal or ethical constraints and opens up new revenue opportunities through the monetisation of aggregated, anonymised, or encrypted insights across sectors.

- Support business expansion into privacy-sensitive markets and regulated sectors (e.g., health, finance, public services)
  PETs allow companies to confidently enter highly regulated domains, such as healthcare or financial services, by ensuring that sensitive data is safely and ethically processed[18]. This reduces legal risk while enabling the development of new services in trust-critical environments.

b) Enhancing brand trust and customer retention in a privacy-first era

With trust as a key modern factor in customer retention, loyalty, and brand reputation, PETs help companies build trust through action, not just policy. According to the survey, while almost one third of the organisations highlighted "increased customer trust" from using PETs, 20% of them have also benefitted from a better brand image, reinforcing PETs potential to act as competitive differentiators.

- Demonstrate ethical use of data, which supports brand differentiation and long-term loyalty
  As underlined in the 2022 GDMA Study[19], consumers are more likely to engage with brands that visibly prioritise their privacy. By adopting PETs, businesses show their

[17] OECD, *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches*, OECD Digital Economy Papers No. 351 (March 2023)
[18] The Royal Society, *From Privacy to Partnership: The Role of Privacy Enhancing Technologies in Data Governance and Collaborative Analysis* (January 2023)
[19] *GDMA, Global Data Privacy, What the Consumer Really Thinks, Foresight Factory*, 2022

commitment to protecting customer data, enhancing their brand image and fostering long-term relationships based on transparency and respect[20].

- Reinforce customer engagement with personalisation that respects privacy boundaries
  With PETs, companies can personalise content and offers based on trends and behaviours, without directly accessing or storing identifiable user data. This leads to improved personalisation[21] while respecting individual privacy preferences and regulatory expectations.

c) Strengthening regulatory resilience and policy alignment

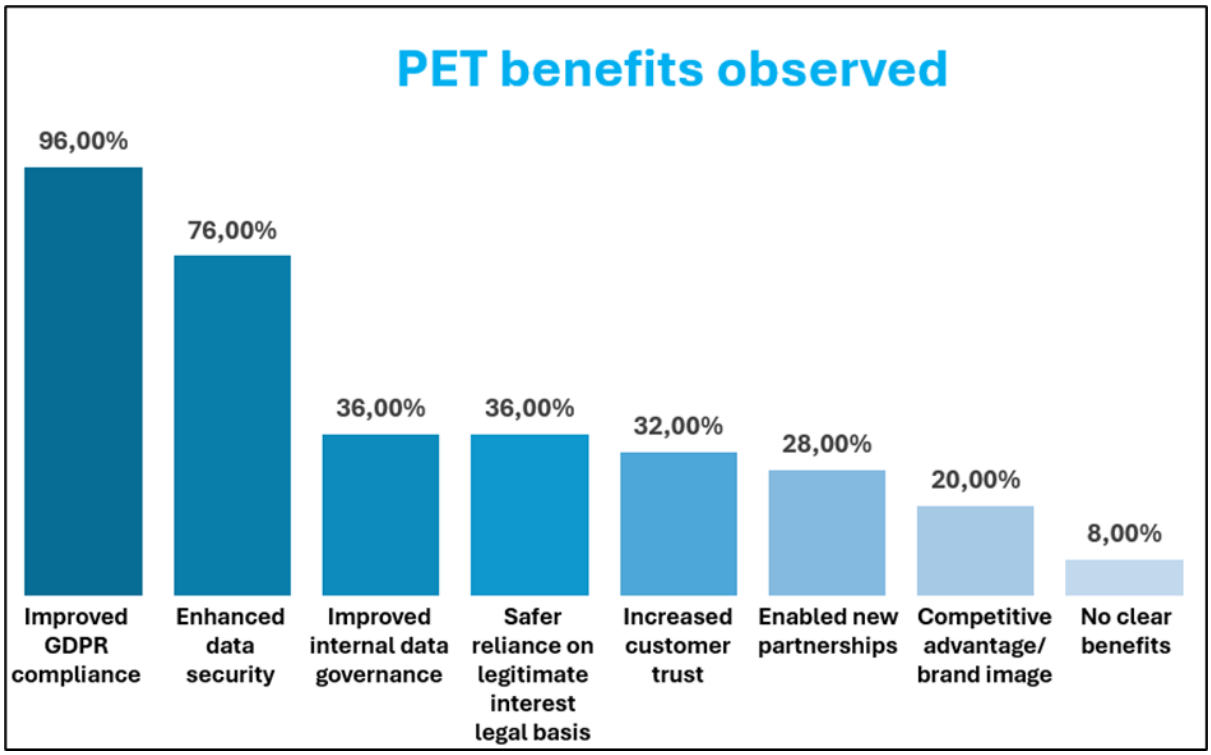
In a rapidly evolving regulatory environment, including the forthcoming Digital Fairness Act proposal, PETs can offer companies a practical way to stay ahead of compliance obligations while achieving internal efficiencies.

- Embed compliance and future-proof operations through technical safeguards
  PETs operationalize core EU data protection principles, such as data minimisation and privacy by design, directly within business systems. This reduces reliance on manual processes, simplifies compliance, and ensures resilience against evolving regulatory requirements and enforcement trends. This is also reflected in FEDMA's survey where 96% of respondents saw improvements in GDPR compliance and enhanced data security (76%) through the use of PETs.

- Reduce legal, reputational, and operational risk while improving efficiency
  36% of the surveyed organisations recognised that the use of PETs has improved their internal data governance. By protecting data throughout its lifecycle, PETs can indeed minimise the risk of breaches and associated costs. They also streamline privacy governance, lower audit and compliance burdens, and enable legally sound innovation in data-driven marketing and services.

[20] *CIPL and CISCO, Business Benefits of Investing in Data Privacy Management Programs*, January 2023

[21] CIPL, *Understanding the Role of PETs and PPTs in the Digital Age* (January 2024)



Question: What benefits has your organisation experienced from using PETs? (Select all that apply)

3.2. Consumers' benefits

a) Enhancing data security and minimising exposure

Consumers are more likely to remain loyal to brands and platforms which take concrete steps to protect their personal data by design. PETs deliver on that expectation by embedding safeguards into the way data is collected, used, and stored throughout its lifecycle.

- Reducing the amount of data exposed or shared, consistent with the GDPR's data minimisation principle
  PETs help limit the personal information being collected or disclosed to only what is strictly necessary, reducing consumers' digital footprint and the risk of unnecessary exposure[22].

- Securing data during processing, through tools like encryption and trusted execution environments
  Even when data needs to be analysed or processed, PETs ensure it remains protected at every step. Techniques such as homomorphic encryption make it harder for unauthorised actors to access or misuse data[23].

[22] Information Commissioner's Office, *ICO Guidance on Privacy Enhancing Technologies (PETs)*, June 2023

[23] OECD, *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches*, OECD Digital Economy Papers No. 351 (March 2023)

- Supporting stronger data governance, ensuring personal information is only used when necessary and in appropriate contexts[24]
  As highlighted in the survey, PETs reinforce internal data governance frameworks by ensuring that access and usage are strictly controlled. This helps organisations prove they are only using personal data in fair, transparent, and lawful ways.

b) Promoting greater user control and confidence

The European Commission's Fitness Check on Consumer Law highlighted that consumers lack the confidence that their choices regarding the use of their data are respected. PETs can empower individuals without overwhelming them.

- Enable meaningful data protection without burdening users with complex privacy choices
  Rather than putting the burden on users to read through lengthy privacy policies, PETs enable built-in privacy protections that work silently in the background.

- Allow privacy-preserving data use on devices, such as smartphones, limiting the need to transmit data externally
  On-device processing enables sensitive operations, like recommendations, to take place locally[25]. This reduces unnecessary data sharing and keeps users in control of their information.

c) Delivering personalised services in a privacy-respecting manner

Consumers appreciate relevance without the risk of compromising on their privacy. PETs ensure that companies can offer tailored experiences without resorting to intrusive tracking or profiling.

- Enabling personalisation through techniques such as federated learning[26] and anonymised insights
  These methods allow companies to refine services based on aggregated patterns, rather than individual user profiles, striking a balance between tailored engagement and ethical data use.

- Making digital experiences more relevant without compromising individual rights[27]
  By embedding privacy into personalisation, PETs help maintain user trust while still delivering convenience and value. This approach reflects the EU's commitment to digital fairness and dignity.

d) Advancing inclusion and ethical data use

Some PETs can help shape a digital environment that is fair, respectful, and inclusive for all individuals, regardless of background or digital literacy.

---

[24] The Royal Society, *From Privacy to Partnership: The Role of Privacy Enhancing Technologies in Data Governance and Collaborative Analysis*, January 2023

[25] Zhang, Yimeng, Mohammad Saeidi, Mahsa Rohanian, Kai Xu, Yifan He, and Helen Christensen, *On-Device Large Language Model Sensing: Personalizing Smartphones Privately and Efficiently*, 2024

[26] CIPL, *Understanding the Role of PETs and PPTs in the Digital Age* (January 2024), p.36.

[27] Laurent, Maryline, Thi-Kim-Ahn Nguyen, Frédéric Cuppens, and Nora Cuppens-Boulahia, A Taxonomy and Evaluation of Privacy Enhancing Technologies for Personalisation, (2023) *Computers & Security*

- Reducing reliance on sensitive data categories that could introduce unintended bias or discrimination[28]
  By limiting the need to process attributes of certain sensitive types of data, PETs such as data clean rooms, reduce the risk of algorithmic bias and help prevent unfair outcomes in areas like advertising, credit scoring, or content curation.

- Enhancing fairness and protection of vulnerable consumers
  PETs, such as pseudonymisation, reduce the risk of exploiting consumers' vulnerabilities by enabling more granular control over data access and usage, thereby preventing the aggregation of extensive personal profiles that could be used to identify and target individuals based on their susceptibilities (e.g., financial distress, health conditions, or psychological traits) for predatory marketing or manipulative practices.

4. Barriers to the broader adoption of PETs

PETs are increasingly recognised for their potential to reconcile data innovation with strong data protection. They promise a path to ethical, compliant, and user-centric data processing, an approach aligned with the values of the GDPR and the EU's digital strategy. However, despite growing interest and technical advancements, the deployment of PETs across industry remains limited. This section explores the key regulatory, technical, business, and governance-related barriers holding back the broader adoption of PETs.

4.1 Regulatory and legal barriers

Despite the recognised potential of PETs to support privacy by design, current EU law and guidance provide few tangible incentives. In particular, recent guidance from the European Data Protection Board (EDPB) presents a complex and, at times, restrictive interpretation of the regulatory landscape for PETs.

- Under ePrivacy (Guidelines 2/2023), the EDPB adopts a broad interpretation of "access" and "storage" on end-user devices[29]. This includes even privacy-preserving operations like generating pseudonymous tokens or conducting local computations. As a result, PETs deployed on terminal equipment may still require prior consent, even when designed to enhance privacy. This undermines the low-friction nature of many PETs and may discourage their use unless very narrow exceptions apply. It also creates a legal divergence where PETs are viewed as safeguards under the GDPR but potentially as intrusive technologies requiring consent under ePrivacy.

- The EDPB's (draft) Guidelines on Legitimate Interests (1/2024) offers a nuanced support to PETs. Though the EDPB explicitly states that PETs reduce risk to data

[28] Mosse Institute of Cybersecurity, *Privacy-Enhancing Technologies: Challenges and considerations*, August 2023, MCSI Library

[29] European Data Protection Board (EDPB), *Gu Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive*, adopted on October 7, 2024, para. 11, 36

subjects and can tip the balancing test in favour of the controller[30], it also makes clear that the lawfulness of processing depends primarily on its purpose and alignment with user expectations, not solely on technical safeguards. This implies that the mere deployment of PETs, which significantly lower the level of risk to data subjects, cannot legitimize allegedly intrusive activities or mitigate data subjects' expectations for a lack of transparency. This limits the role of PETs in legitimising broader data use cases.

- The EDPB's Guidelines 01/2025 on Pseudonymisation recognise pseudonymisation as a valuable support to GDPR's core principles[31]. However, they also set a very high bar for effectiveness, requiring strict key separation and consideration of contextual re-identification risks[32], which many real-world PET implementations may not meet. Even though the current EDPB Guidelines reaffirm that pseudonymised data remains personal data, even if re-identification keys are held separately[33], the recent EUCJ SRB case (see EDPS v SRB C-413/23P) confirmed that pseudonymised data held by a processor without reasonable means to reidentify the dataset (i.e. the key remains with the controller) should not be considered personal data. As a result, the European Commission's Digital Omnibus proposal has reflected the relative approach to anonymity (as ruled in the SRB case) by amending Article 4 of the GDPR, and introduced a mandate for an implementing act to define criteria for determining when pseudonymised data is no longer considered personal data. These opposing views create confusion and uncertainty on the current and future state of affairs, understandably leading to investment and deployment reluctance. The situation is moving fast, following the EDPB's stakeholder event on the 12th of December 2025 to gather perspectives on the implications of the SRB case on its guidelines on pseudonymisation, as well as the leading parties in the SRB case withdrawing the proceedings before the General Court which agreed to close the case without further clarifications.. The revised EDPB Guidelines and the potential codification of the tenants of the SRB case in the Digital Omnibus should clarify the situation and stimulate the deployment of pseudonymisation (and other PETs).
- Until now, contextual advertising has been the only advertising model supported by EU policymakers and regulators in official documents, such as the European Commission's Cookie Pledge proposal and the EDPB's Opinion on Pay or Consent[34] for Large Online Platforms. These texts have positioned contextual advertising as the most favorite alternative to personalised models. However, this regulatory preference has been widely criticised for overlooking the reality that contextual advertising is not commercially viable for many economic actors. The absence of any official endorsement or recognition of PET-based advertising solutions, which are specifically designed to reduce or eliminate the privacy risks associated with data-driven

[30] European Data Protection Board (EDPB), *Guidelines 01/2024 on the Processing of Personal Data under Article 6(1)(f) GDPR*, adopted on February 13, 2024, para. 56

[31] European Data Protection Board (EDPB), *Guidelines 01/2025 on Pseudonymisation*, adopted on January 16, 2025, pp. 10, 13-16

[32] European Data Protection Board (EDPB), *Guidelines 01/2025 on Pseudonymisation*, adopted on January 16, 2025, para. 21, 22

[33] European Data Protection Board (EDPB), *Guidelines 01/2025 on Pseudonymisation*, adopted on January 16, 2025, para. 16, 18, 20

[34] European Data Protection Board (EDPB), Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, adopted on April 17, 2024, para.75

marketing, has artificially narrowed the policy debate to a false dichotomy between contextual and personalised advertising.

Together, these gaps send a mixed signal to the industry: while PETs are encouraged in principle, at a policy-level, the uncertain regulatory environment and the limited consideration of operational realities are not supportive of PETs deployment in practice.

4.2 Informational and operational barriers

- **Implementation complexity and lack of standards**
  Many PETs, such as secure multi-party computation or homomorphic encryption, are technically complex, requiring advanced expertise, computational power, and changes to IT infrastructure. These demands pose a substantial challenge—particularly for organisations lacking dedicated privacy engineering teams. Survey data confirms this: over 40% of respondents cited lack of awareness or understanding of PETs, and an equal share were not aware of available PET providers or tools, highlighting that informational barriers are the most common obstacles to adoption. Additionally, more than 20% pointed to a lack of internal technical expertise, and 26.7% flagged the difficulty of integrating PETs into current systems as a major operational concern. The absence of unified standards across industry and regulatory bodies further compounds these challenges, creating interoperability risks and reducing confidence in PETs. However, there are positive developments regarding the standardisation of certain PETs, such as IAB Tech Lab's Working Group on PETs[35]. The recent SRB Case mentioned above presents a significant win for pseudonymisation and could by extension help promote PETs overall, especially as the Digital Omnibus proposal codifies the SRB ruling and aims at providing criteria for when pseudonymised data is no longer considered personal data.

- **Performance and usability trade-offs**
  In some cases, PETs may reduce the utility of data or degrade performance due to encryption, latency, or limits on granularity. Where PETs reduce analytical accuracy or complicate existing workflows, adoption is deprioritised, especially in data-driven sectors like marketing, finance, and health.

4.3 Economic and market barriers

- **Cost and return on investment (ROI)**
  Without regulatory incentives or market recognition, some businesses may favour less privacy-friendly but commercially proven tools. 26.7% of surveyed organisations cite the lack of a clear business case or ROI, and high adoption costs as the main barriers for not using PETs. These technologies often involve high upfront costs, including R&D, licensing, staff training, and infrastructure upgrades. These costs are especially burdensome for SMEs and start-ups, which lack the scale to absorb them easily. At

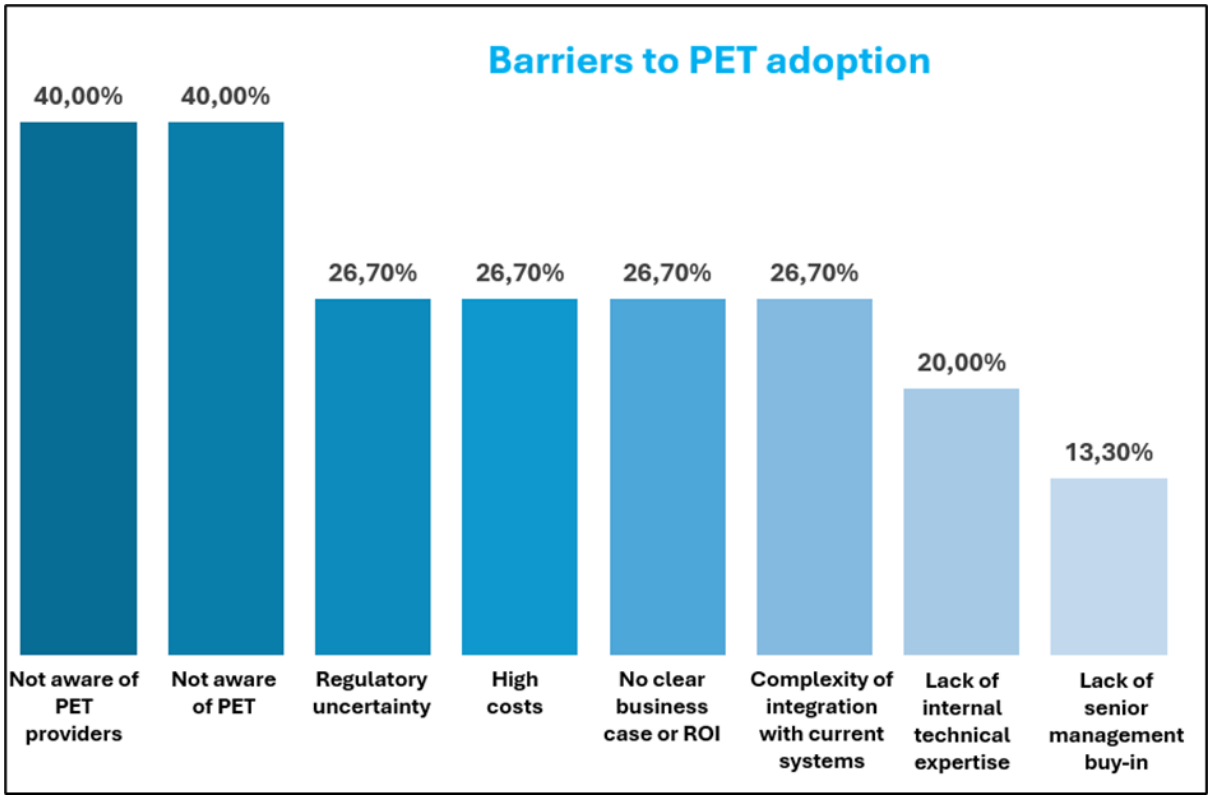
[35] IAB Tech Lab https://iabtechlab.com/working-groups/rearc-addressability-and-privacy-enhancing-technologies-pets-working-group/

the same time, the return on investment is difficult to quantify. While PETs reduce risk and enhance trust, these benefits are hard to monetise directly.

4.4 Organisational and governance barriers

- **Knowledge gaps and siloed responsibilities**
  PETs require collaboration between legal, technical, and business functions. Yet in many organisations, these teams operate in silos. Engineers may not fully understand data protection requirements, while legal teams may lack the technical fluency to evaluate PETs. The result is an implementation gap: even when PETs are technically available, they are not fully deployed or integrated into broader privacy strategies.

- **Limited regulator readiness**
  Regulators themselves face capacity constraints. PETs often involve complex cryptographic methods, emerging computing paradigms, or context-specific threat modelling. Without internal expertise, regulators may hesitate to endorse specific PET implementations



Question: What are the main reasons your organisation is not currently using PETs or not scaling their use? (Select all that apply)

5. Policy recommendations for supporting the development and adoption of PETs

The successful development and widespread adoption of Privacy Enhancing Technologies (PETs) will require close collaboration between industry and policymakers. While industry must lead in integrating PETs into operational, technical, and business practices, public authorities play a critical role in creating the legal, regulatory, and economic conditions that make adoption viable at scale. These efforts are complementary and mutually reinforcing: only by working together can both sides ensure that PETs fulfil their promise of enabling privacy-respectful innovation in Europe's digital economy. The following recommendations outline specific actions each stakeholder group can take to advance this shared goal.

5.1 Recommendations for Industry

a) Leverage industry standards, labels, and certifications to build trust

Industry actors should actively participate in national, European, and international standardisation initiatives (e.g. CEN/CENELEC, ISO/IEC, ETSI, IAB Tech Lab) to help define interoperable, scalable, and sector-specific PET standards. This includes contributing to emerging frameworks on federated analytics, data clean rooms, anonymisation techniques, cryptographic PETs, as well as standards for integrating PETs into broader privacy governance frameworks, demonstrating their use, applying assurance mechanisms, and methodologies to assess PET effectiveness and ROI. Survey data confirms the relevance of this approach: 48% of respondents said that industry standards would encourage them to adopt or scale up PETs, highlighting the role of standardisation in building trust, reducing fragmentation, and facilitating adoption.

- **Why this matters**: Without common standards, PET solutions remain fragmented, difficult to integrate, and challenging to scale across the data economy.

The development of standards, trust labels, and certification schemes to define what constitutes a Privacy Enhancing Technology (PET), how it is implemented, and what level of protection it offers can help inform consumers, regulators, and business partners about the functionality and limitations of PETs, distinguishing robust privacy-preserving solutions from superficial claims. This is essential not only to counter the growing risk of "privacy washing," but also to foster meaningful adoption. In fact, 60% of survey respondents indicated that guarantees about consumer trust and reputational benefits would encourage them to adopt or scale up PETs, underscoring the value of trusted signals in building confidence around PET-enabled marketing practices.This will be essential to build public trust in PET-enabled marketing practices and to address the growing risk of "privacy washing", where companies overstate privacy protections without delivering meaningful safeguards or accountability.

- **Why this matters**: Without clear definitions and trusted signals, consumer trust may be undermined, and legitimate PET efforts could be overshadowed by misleading or unverified claims.

b) Implement privacy frameworks

Companies should integrate PETs within broader privacy-by-design and data governance frameworks, aligned with GDPR principles and the direction set by the Digital Omnibus and

the implementing act which aims at specifying which criteria for when pseudonymised data is no longer considered personal data. Adopting internal PET policies and embedding them in compliance, procurement, and product development cycles ensures consistency and accountability. For instance, companies have policies that all data where clear-text use is not necessary, must be pseudonymised the moment data is received. PETs are used to automate this first step before any file can enter into a filing system (for instance to be part of a CRM). This makes the use of data for analytics, for instance, carry less processing risk. Where corporate entities have multiple legal persons, the pseudonymisation effort can be seen as "anonymisation", provided that appropriate safeguard against re-identification are made.

- **Why this matters**: PETs are most effective when embedded in governance structures—not as ad hoc tools, but as strategic privacy enablers.

c) Document and demonstrate PET use

Organisations should document how PETs are applied across use cases, e.g., segmentation, analytics, cross-party collaboration, and under which legal bases. Clear internal records and external transparency (e.g. in DPIAs, records of processing activities, privacy notices) help build trust with customers, partners, and regulators.

- **Why this matters:** Demonstrating PET use is essential for accountability, defensible compliance, and strengthening credibility with stakeholders.

d) Adopt assurance mechanisms

To foster confidence in PET implementations, companies should adopt technical and organisational assurance mechanisms. These include:

- Independent audits
- Logging and access control
- Certification (when available)
- Use of formal verification and cryptographic proofs

Such measures help verify that PETs deliver on their privacy promises and mitigate regulatory and reputational risks.

- **Why this matters**: Assurance mechanisms provide the verifiability needed to move from trust to trustworthiness, especially under regulatory scrutiny.

e) Establish methodologies to assess PET effectiveness and ROI

Industry should work collaboratively, across privacy, technical, and business teams, to develop practical methodologies and criteria to assess the effectiveness, performance, and return on investment (ROI) of PETs. This includes defining metrics to evaluate privacy protection (e.g. reidentification risk reduction), business impact (e.g. campaign performance, customer trust), and operational feasibility (e.g. integration cost, resource needs).

- **Why this matters**: Without clear ways to measure effectiveness, PETs may struggle to gain internal buy-in or scale beyond pilots, especially among SMEs and non-technical decision-makers.

5.2 Recommendations for Policymakers

a) Develop and align standards

The European Commission and Member States should support the development and convergence of technical and organisational standards for PETs across sectors and use cases. This includes active engagement in European standardisation processes (e.g. through CEN/CENELEC technical committees or joint working groups with ETSI and ISO/IEC) to define interoperable, secure, and auditable PET implementations. Where relevant, these standards should connect with GDPR codes of conduct (Article 40), certification mechanisms (Article 42), AI governance frameworks, and interoperability principles. As mentioned earlier, 48% of survey respondents identified industry standards as a key incentive to adopt or scale up PETs, highlighting the practical need for clearer, authoritative guidance to enable confident and consistent deployment.

- **Why this matters**: Harmonised technical and legal standards make PET adoption more predictable, scalable, and trustworthy across the EU, especially for cross-border data processing and smaller actors needing guidance.

b) Provide clear legal guidance

To support broader adoption of PETs, EU policymakers and Data Protection Authorities (DPAs) should issue detailed, practical, and harmonised guidance on how PETs align with key GDPR concepts, such as anonymisation, legal bases, and accountability. As mentioned in section 4.1, legal uncertainty in these areas remains a major barrier to implementation. This is strongly echoed in the survey findings: 72% of respondents indicated that clear guidance from DPAs on the compatibility of PETs with GDPR would encourage them to adopt or scale up these technologies. Such clarity would help organisations navigate compliance obligations with greater confidence, while also preventing inconsistent interpretations across Member States that could hinder cross-border applications of PETs. The following areas require particular attention:

- <u>Legitimate interest assessments:</u>

FEDMA's survey showed that clarity on how PETs can strengthen the case for legitimate interest under Article 6(1)(f) GDPR would incentivize broader PET adoption for 52% of respondents. Guidance would be necessary, particularly when used to reduce the risks associated to certain data processing or in data processing that might otherwise require consent under the existing ePrivacy framework, including:

- Audience measurement
- Attribution and analytics
- Data collaboration in marketing partnerships

Additionally, regulatory guidance should clarify that when a specific PET demonstrably and significantly reduces the risk to the rights and freedoms of data subjects, this technical safeguard, which carries substantial weight in the legitimate interest assessment, can potentially outweigh subjective user expectations. In such cases, the objective reduction of harm through PETs can justify data processing even where individuals may not fully anticipate the specific use, provided transparency and accountability measures are in place.

- **Why this matters**: Many companies struggle to justify legitimate interest in light of GDPR and ePrivacy restrictions. PETs could offer a path forward, but only if this is explicitly acknowledged.

❖ Anonymisation vs. Pseudonymisation

Regulators should provide guidance on : (a) when data processed using PETs (e.g., through aggregation, differential privacy, or secure computation) can be considered anonymised or pseudonymised in such a way that it falls outside of the scope of the GDPR for a given party which has no reasonable means to re-identify individuals; and concurrently, (b) when such processed data should still be treated as personal data requiring compliance with the GDPR . This includes clarification of thresholds, conditions, and risk assessment criteria for robust anonymisation in different PET implementations.

- **Why this matters**: Companies hesitate to deploy PETs due to uncertainty over whether the resulting data still triggers GDPR compliance.

❖ Joint controllership

- Provide clarity on how joint controllership or processor-controller relationships should be determined in federated learning, data clean rooms, and MPC-based collaborations. This need for clarity becomes even more relevant as there are different stages of processing, including stages in which data can be treated as anonymous.
- Include model contract clauses or accountability checklists to help organisations allocate obligations (e.g., who performs DPIA, handles access requests, or ensures transparency).

- **Why this matters**: PETs often involve data processing across organisational boundaries, but the GDPR responsibilities in these distributed models remain unclear.

❖ Secondary data use and purpose limitation

- Provide guidance on how PETs can enable responsible secondary uses of personal data while staying within the original purpose or remaining compatible with it.
- Specify how the use of privacy-preserving aggregation or encryption affects the assessment of purpose compatibility under Article 5(1)(b) GDPR.

- **Why this matters**: Many companies see value in data reuse but are unclear on how PETs can enable this while remaining compliant.

c) Support innovation through regulatory sandboxes

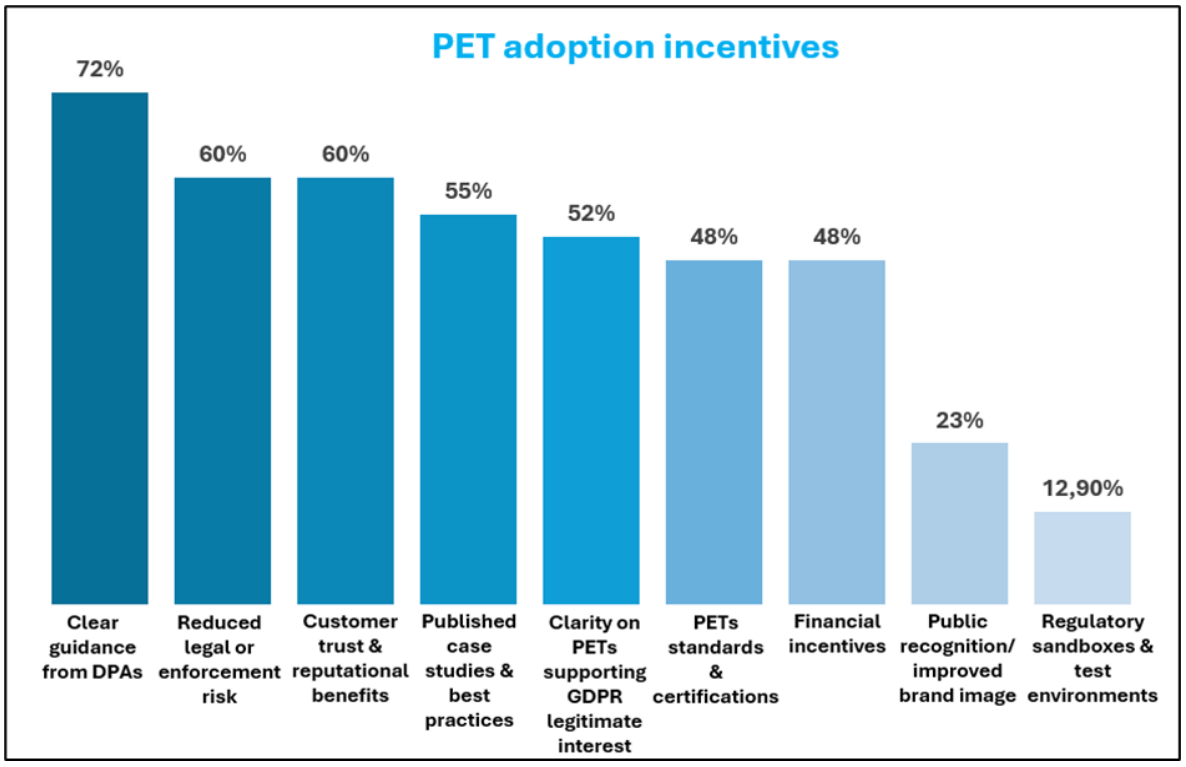
National Data Protection Authorities (DPAs), in collaboration with innovation agencies, should establish regulatory sandboxes for testing PETs in real-world settings. Such environments can offer legal clarity, co-regulatory dialogue, and faster deployment of compliant solutions.

- **Why this matters**: Sandboxes create a safe space for experimentation, enabling businesses, especially SMEs, to develop PET solutions without fear of non-compliance or enforcement.

d) Incentivize and endorse PET adoption

The use of certified or well-documented PETs should be officially recognised as a mitigating factor in supervisory actions or enforcement decisions under GDPR. Policymakers could also explore financial incentives, such as innovation grants or public procurement criteria favouring PET-based solutions, especially for SMEs. Importantly, 60% of survey respondents stated that guarantees around reduced legal and enforcement risks would encourage them to adopt or scale up PETs, highlighting how regulatory endorsement can play a critical role in de-risking investment. As mentioned in Section 5(a), the lack of official recognition or endorsement of PET-based advertising solutions, which are specifically designed to mitigate or eliminate privacy risks in data-driven marketing, has artificially constrained the policy debate to a false binary between contextual and tracking-based advertising. To move beyond this limited framing, we recommend that EU policymakers and regulators formally acknowledge and support PET-based advertising models as credible, privacy-preserving alternatives that allow innovation, consumer protection, and regulatory compliance to go hand in hand.

- **Why this matters**: While strategic incentives can accelerate PET uptake by reducing legal risk, lowering cost barriers, and rewarding privacy leadership, without policy-level recognition, privacy-preserving innovation risks being stifled, and the EU may miss the opportunity to shape a digital advertising ecosystem that is both privacy-respectful and economically sustainable.



Question: What kind of legal or regulatory certainty would support broader PET adoption? (Select all that apply)

6. Conclusion - Unlocking the potential of PETs in marketing and advertising

Privacy-Enhancing Technologies (PETs) are increasingly recognised as essential tools for reconciling data-driven innovation with privacy and regulatory compliance. While basic PETs like pseudonymisation are widely used, advanced techniques such as federated learning and secure multiparty computation remain underutilised, despite their promising features. The strategic potential of PETs—beyond compliance—is still largely untapped, with few organisations viewing them as drivers of brand value or competitive differentiation.

FEDMA organised an industry workshop in June 2025 to explore the opportunities and challenges of Privacy Enhancing Technologies (PETs) in the advertising and marketing ecosystem. Our workshop, combined with our industry survey reveal that:

1. PET adoption is primarily compliance-driven.
2. Lack of awareness, legal clarity, and integration challenges are major barriers.
3. There is strong demand for practical guidance, training, and implementation support.

The Need for Multi-Stakeholder Collaboration

Effective PET deployment requires coordinated efforts across industry, regulators, civil society, and academia. The FEDMA-Google workshop emphasised the importance of aligning business incentives with privacy goals, and avoiding “privacy washing” by ensuring transparency and accountability.

Key collaboration imperatives include:

- **Policy alignment**: we call on regulators to provide clear legal frameworks and/or guidelines that support PET integration into privacy-by-design models.
- **Standardisation**: incentivise industry actors to engage in developing interoperable PET standards through bodies like ISO, IAB Tech Lab, CEN/CENELEC, and ETSI.
- **Civil society engagement**: Involving NGOs and consumer advocates ensures PETs address real-world privacy concerns and build public trust.

Next Steps for Fostering PET Adoption

Looking forward, in order to accelerate PET uptake in digital marketing, the following actions are recommended:

- **Develop sector-specific implementation guides**: Tailored resources for marketers, SMEs, and tech platforms to demystify PETs and facilitate integration.

- **Launch pilot programs**: Showcase real-world use cases demonstrating ROI, legal robustness, and consumer benefits.
- **Create shared governance frameworks**: Encourage documentation of PET use in DPIAs, privacy notices, records of processing activities and internal records to foster transparency and regulatory confidence.
- **Support training and capacity-building**: Equip marketing professionals and compliance teams with the skills to evaluate, deploy, and manage PETs effectively.

FEDMA will aim for continued engagement with policymakers and civil society to ensure the legislative framework reflects a balanced approach - one that promotes innovation while protecting fundamental rights. In the spirit of collaboration and openness, we welcome comments, questions or any stakeholder feedback that can help advance the cause of PETs.

About FEDMA

The Federation of European Data & Marketing (FEDMA) is a respected and influential advocacy trade association in Brussels representing all matters related to privacy, consumer protection and data-driven marketing. Our objective is to promote and protect the European data driven marketing industry by creating greater acceptance and usage of data marketing by European consumers and business communities. FEDMA develops ethical standards for the industry to ensure greater consumer trust, and fights for the freedom of communication by encouraging European institutions to ensure a healthy commercial and legislative environment within which the industry may operate and develop.