Trusted Execution Environments in Digital Advertising:

A Pathway to Enhanced Data Privacy, Security, and Regulatory Compliance

iab.

April 2025

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

A. PURPOSE

In today's connected world, prioritizing privacy and data security is essential for companies to maintain public trust. As global regulations evolve, organizations must responsibly manage data and address privacy and security as default when developing their products. This is why the future of digital advertising must balance innovation with privacy, using new technologies that protect data while allowing consumers to benefit from the free, ad-supported Internet. This white paper provides an overview of Trusted Execution Environments (TEEs), their role as a privacy-enhancing technology (PET), and their application in the digital advertising industry. It explores how TEEs strengthen data protection, security, and privacy while providing policymakers and regulators with insights into their benefits, challenges, and potential regulatory implications. Additionally, it highlights opportunities to incentivize the development, adoption, and use of TEEs to improve consumer data protection.

TEEs, a type of PET, are isolated and secure confidential computing spaces for data processing that are verifiable and auditable. They enhance data protection, security, and privacy in digital advertising. For example, TEEs can be used to improve data clean rooms, help make good on assurances to customers, decrease data privacy and security risks, and align data processing with key principles in regulations like the General Data Protection Regulation (GDPR) and U.S. state privacy laws.

Incentivizing the digital advertising ecosystem to develop, adopt, and use TEEs will result in greater use, leading to widespread data protection benefits. It also addresses a crucial market reality: research shows that 80% of consumers still prefer relevant advertising, which requires some level of personalization. TEEs offer a path forward that enhances data security and promotes key privacy principles while supporting businesses' ability to deliver relevant experiences that their customers prefer. This is particularly important for smaller enterprises that rely on digital marketing to reach customers by leveraging their first-party data. TEEs offer technology protections to such customers.

[1] https://www.iab.com/news/consumer-privacy-research/

B. KEY TAKEAWAYS

- **Enhanced Data Privacy and Security:** TEEs protect user data by enabling processing in isolated and secure environments, minimizing the risk of unauthorized access and processing, and reducing data leakage. TEEs also provide verifiable proof that code runs securely and meets compliance standards, ensuring accountability and trust for regulators and data controllers.

- **Regulatory Compliance:** TEEs promote both technical and practical compliance with several key principles upon which data protection laws are built–i.e., data minimization, privacy-by-default, purpose limitation, and accountability.

- **Opportunities for Policy Support:** Policymakers can play a critical role in encouraging the adoption of TEEs and other privacy-enhancing technologies. In doing so, they can foster a privacy-responsible digital ecosystem.

II. THE ROLE OF CONFIDENTIAL COMPUTING AND TEES IN DIGITAL ADVERTISING

A. BACKGROUND OF TEES AND THEIR BENEFITS

Confidential computing through hardware-based TEEs establishes higher standards for data protection due to the protections it provides to processed data. They are widely used in cloud computing, digital advertising, and financial services to enhance privacy and security.

In particular, TEEs provide a secure area within a processor for executing code and processing data without exposure to the broader system. TEEs prevent unauthorized access to data, even from the operating system or other applications, ensuring confidentiality and integrity. When coupled with encryption and other PETs, TEEs further restrict data from unauthorized access. Even system administrators cannot access the data, creating a trustworthy setup for handling personal information.

Additionally, TEEs use secure cryptographic methods to prove they meet strict security standards for running code. Independent organizations can verify and audit this, ensuring for data controllers and regulators that the data is being handled safely.

CORE BENEFITS FOR PRIVACY AND SECURITY

- **Data Isolation:** TEEs provide robust protection for consumer data by enabling isolated processing environments, significantly reducing the risk of unauthorized access. For example, TEEs have long been used for secure payment processing and digital rights management where privacy and security are of the utmost importance. Today, TEEs can also be utilized by publishers and advertisers for campaign activation against their customer information without disclosing the underlying raw data.

- **Verifiable Compliance:** This process verifies that a TEE's setup stays secure and unchanged (using cryptographic technologies), ensuring that data remains protected and trustworthy.[2]

- **Alignment with Regulatory Principles:** TEEs support regulatory privacy principles, such as privacy-by-default, data minimization and purpose limitation, by allowing data to be processed securely without extensive data transfer or exposure. They also promote accountability through the attestation process described in this paper.

- **Data Confidentiality Throughout the Lifecycle:** Data remains protected even during processing within the TEE. For instance, for data analytics and measurement use cases in digital advertising, where the output data is typically included in aggregated or de-identified reports, TEEs enable parties to compute the data without revealing underlying raw data to each other.

- **Verification of Trust:** Attestation, a feature of confidential computing, allows for auditing and verification of the TEE's integrity and the software running within it. This combination of isolation and attestation ensures that data remains confidential and protected from unauthorized access, including by system managers, addressing a crucial vulnerability in traditional data security.

[2] Confidential computing is a PET that relies upon TEEs. The benefits of TEEs should be compared to other types of PETs, which is set forth in Appendix A.

The chart below examines how TEEs offer enhanced data protection compared to processing without that technology.

Comparing Traditional Processing and TEE-Protected Processing

Feature	Processing Without TEEs	TEE-Protected Data Processing
Data Handling	Raw user data may flow through multiple systems	User data processed in isolated secure hardware enclaves
Access Control	System administrators, cloud providers, and partners can potentially access raw data	Even system administrators cannot access data within a TEE
Security Level	Protection primarily through access policies and encryption at rest/transit	Hardware-level protection with cryptographic isolation during processing
Verification	Limited auditability of data access and processing	Cryptographic attestation verifies the integrity of processing environment
Data Protection	Data protection is contractually guaranteed	Significantly reduced risk, as raw data remains protected
Privacy and Regulatory Alignment	Data minimization and purpose limitation are business-driven decisions (e.g., whether to apply PETs)	Enhanced data minimization and purpose limitation controls
Cross-Border Transfers	Represents a heightened transfer risk if raw data is involved	Can mitigate concerns through verifiable processing controls

B. USE CASES FOR TEES IN DIGITAL ADVERTISING

TEEs not only support regulatory transparency and accountability; they also create a secure, verifiable data processing environment that supports commercial transparency and accountability. Importantly, this technology allows small and medium-sized businesses (SMBs) to participate in privacy-focused digital advertising without compromising security or compliance, fostering a competitive and trustworthy digital advertising market. This environment also ensures that data processing actions can be audited and verified, enabling advertisers and regulators to confirm that data handling aligns with privacy standards and commercial priorities. Key digital advertising products utilizing TEEs include:

- **Google's Confidential Matching:** Allows advertisers to securely connect their first-party data for measurement and audience solutions. Customer information is processed in a manner that is secure by default. Other technical assurances include transparency into a product's code and the ability to receive attested proof that data is processed as intended.

- **Microsoft Azure's Confidential Computing for Clean Rooms:** Microsoft uses TEEs to create "data clean rooms" in its Azure environment. Used together with other PETs, such as encryption, these secure spaces allow advertisers to share and analyze data without exposing each party's underlying raw personal information.

- **Amazon Web Services (AWS) Nitro Enclaves:** A feature within AWS that leverages TEEs to create highly isolated, secure "enclaves" where sensitive data can be processed and computed without exposure to the broader cloud environment, even from the host operating system or AWS itself. It provides a strong layer of confidentiality and integrity for sensitive applications.

III. POLICY IMPLICATIONS AND CONSIDERATIONS

A. POLICY CONTEXT: DIGITAL ADVERTISING'S PRIVACY AND SECURITY PARADIGM

The global privacy landscape is evolving rapidly as governments respond to growing public concerns about how information is used and shared online. This regulatory movement reflects a fundamental shift in how we view personal information in the digital age.

While approaches vary across jurisdictions—from Europe's GDPR approach that requires a legal basis to process personal data to U.S. states' focus on governing the sale or sharing of personal information—they share common objectives: providing transparency, promoting privacy by default approaches to product development, limiting unnecessary data leakage and propagation, and protecting vulnerable populations.

TEEs have emerged as a critical solution to the complex challenge of meeting important consumer privacy obligations and digital advertising business objectives that support the free and open Internet. Adoption of TEEs represents a significant advancement for the digital advertising industry. By supporting certain verifiable and auditable privacy and security protections, TEEs create valuable opportunities for businesses of all sizes to protect customer data transparently, which builds trust and promotes transparency in digital advertising. It also establishes verifiable certification of data protection that benefits both companies and consumers, which is tied to data protection principles.

The growing adoption of technologies like TEEs represents a promising direction – one that can enhance meeting regulatory requirements while maintaining the economic benefits of responsible data use in advertising.

B. SUPPORTING COMPLIANCE WITH DATA PROTECTION LAWS

TEEs, by isolating data processing and enabling cryptographic verification, offer technical capabilities to enhance data security and promote compliance with privacy requirements such as purpose limitation, data minimization, and partner accountability. This alignment is crucial for organizations facing compliance obligations under laws such as the GDPR and U.S. state privacy laws, which demand high data protection and accountability standards.

[3] PETs, as defined by authorities like the National Science and Technology Council, enable valuable data insights while protecting personal information. Their importance is recognized by regulatory bodies worldwide, including the **UK's Information Commissioner's Office**, the EU (through GDPR provisions on data minimization privacy by design and purpose limitation), and the CNIL (through its latest **strategic plan**).

For policymakers seeking approaches that balance privacy, security, and economic utility, TEEs create a middle path that protects personal information while supporting basic targeted advertising use cases that support a free ad-supported Internet. Indeed, hardware-based protections establish stronger safeguards than purely policy-based controls, as they physically constrain how data can be accessed.

1. KEY REGULATORY BENEFITS

TEEs enhance public policy goals related to data protection. Their architecture directly supports key regulatory principles in several important ways:

- **Privacy-By-Default:** TEEs protect personal data automatically when they are being processed in confidential compute enclaves. They isolate and secure data in a way that prevents unauthorized access, meaning that privacy is built into the system from the start, without requiring additional measures or user intervention. This is the type of privacy-by-default product design envisioned in regulations like GDPR that prioritizes consumer safety first.
- **Transparency and Accountability:** TEEs provide regulators and data controllers with cryptographic logs that enable verifiable audits of data processing actions. This accountability feature transforms abstract compliance requirements into technically enforceable guarantees. In particular, it promotes the efficiency and scalability of service provider assessments, which are widely required under privacy laws.
- **Cross-Border Data Transfers:** Given the complexity of cross-border data transfer regulations, TEEs offer a technical solution to mitigate some associated risks. By keeping data secure during processing and preventing unauthorized access, TEEs can support compliance with instruments like the EU's Standard Contractual Clauses and Binding Corporate Rules, if a company uses one of those instruments. Additionally, TEEs' isolation of data processing helps address concerns about unauthorized data access in foreign jurisdictions, as required by the Schrems II decision on transatlantic data transfers.
- **Purpose Limitation:** TEEs protect raw data from secondary uses that are inconsistent with the consumer's reasonable expectations and promises that the controller may have made to the consumer concerning the use of such information.
- **Data Minimization**: By isolating data processing in secure enclaves, TEEs enhance data minimization. They keep raw data from being further propagated into other systems, while allowing necessary processing and enabling heightened access control to minimize data leakage. These features help businesses comply with foundational privacy principles without sacrificing analytical capabilities that drive economic value.

2. CHALLENGES AND CONSIDERATIONS

Despite their promise, TEEs have practical considerations for regulators and industry stakeholders. Implementing TEEs across advertising networks requires infrastructure investment, and not all organizations may have immediate access to TEE-compatible hardware. Additionally, ensuring data protection across jurisdictions involves complex configurations, especially for multinational entities handling diverse data sources. Policymakers should consider these limitations when evaluating TEE adoption and develop guidelines that recognize such constraints while encouraging gradual implementation.

IV. RECOMMENDATIONS FOR POLICYMAKERS AND REGULATORS

Policymakers can play an important role by incorporating privacy-enhancing technologies, such as confidential computing, into regulatory frameworks. Incentivizing the use of these technologies will likely accelerate their adoption while advancing data protection and economic development. This balanced approach supports a trustworthy digital ecosystem that respects user privacy while enabling responsible innovation.

By incorporating TEE requirements or incentives into regulatory frameworks, policymakers can establish outcome-based standards that protect privacy through verifiable technical means rather than by prescriptive rules that may quickly become outdated.

A. ENCOURAGING TEE ADOPTION IN ADVERTISING

Policymakers can foster the adoption of TEEs across the digital advertising ecosystem by creating incentives and frameworks that support TEE deployment. This could involve providing grants or subsidies for organizations adopting privacy-enhancing technologies, especially SMBs that may face financial barriers. Additionally, public-private partnerships could help accelerate TEE integration, allowing policymakers and industry stakeholders to collaboratively shape best practices.

B. ESTABLISHING STANDARDS AND BEST PRACTICES

To ensure consistent and effective implementation of TEEs, regulatory bodies could work with industry leaders and technology experts to establish standards that align with privacy regulations. These standards would clarify technical specifications, data management requirements, and security protocols necessary to make TEEs an effective component of a privacy-compliant advertising ecosystem. By providing a structured framework for TEE usage, regulators can help create uniformity and raise confidence in TEEs as a privacy solution.

C. POTENTIAL FOR TEE-SUPPORTED CERTIFICATION PROGRAMS

Certification programs could serve as an additional layer of accountability and trust for organizations that adopt TEEs. Regulatory bodies could partner with certification organizations to develop programs that assess and certify the privacy and security capabilities of TEE-enabled advertising technologies. This certification could provide advertisers with a recognizable mark of compliance, making it easier for consumers and regulators to identify platforms that prioritize data protection. Such programs would further incentivize TEE adoption by distinguishing privacy-conscious brands in the market.

V. CONCLUSION: THE FUTURE OF TEES IN PRIVACY-FOCUSED DIGITAL ADVERTISING

This white paper has outlined how TEEs can address the dual goals of promoting privacy and security and enabling innovation in digital advertising. By securely isolating data processing and offering cryptographic attestation, TEEs enhance data protection and key privacy principles that undergird data protection laws. Doing so promotes trust between consumers, advertisers, and regulators.

As privacy regulations continue to reshape the digital advertising landscape, TEEs offer a scalable and technically robust solution for secure data processing. However, the future of TEEs in advertising will depend on continued investment, cross-industry collaboration, and thoughtful regulatory support. Policymakers have the opportunity to encourage this transformation by supporting research, standardizing best practices, and enabling certification programs that make it easier for organizations to adopt TEEs responsibly.

By facilitating the responsible use of TEEs in digital advertising, regulators can ensure that privacy protections keep pace with technological innovation, fostering a safer and more trustworthy digital environment for all.

APPENDIX A

Comparing TEEs to Other Processing Models

Feature	TEE	Multi-Party Computing	On Device Processing
Data Access Control	Raw data is inaccessible from outside of the enclave	Does not reveal data held by the other party	Data is not centrally shared
Processing Location	Can be decentralized or within hardware-protected secure enclave	Decentralized processing	Decentralized processing
Security Level	Data is decrypted but processed within a secure enclave	Data is never decrypted Not a verified, attested environment.	Data may or may not be encrypted but stays within each device
Scalability	Scalable if supported with sufficient hardware. Easier for parties to implement based on the common server code	Rely on decentralized devices to compute and has limited scalability. More complicated implementation process for parties to adopt	Rely on decentralized devices to compute and has limited scalability
Associated Cost	Cost of hardware	Applies multiple layers of encryption, which can be more expensive than TEE-based processing	Limited additional cost

Interactive Advertising Bureau, Inc. ("IAB") provides this whitepaper as a resource for general information. Please be aware that this whitepaper does not constitute legal advice, and if you have any legal questions, please consult your attorney. While IAB has made efforts to assure the accuracy of the material in this whitepaper, it should not be treated as a basis for formulating business and legal decisions without individualized legal advice.

IAB makes no representations or warranties, express or implied, as to the completeness, correctness, or utility of the information contained in this whitepaper and assumes no liability of any kind whatsoever resulting from the use or reliance upon its contents.