CONTRIBUTION OF ID side to EDPB PUBLIC CONSULTATION on

Guidelines 01/2025 on Pseudonymisation

1. Our Organization in a nutshell

ID side is a French independent start-up created in 2019, right after the adoption of the GDPR in EU, by 3 associates: an expert in Privacy (Marie-Charlotte Roques-Bonnet, 20 years' experience), an expert in Security (Alain Pannetrat, 20 years' experience) and a Data visualisation expert (Damien Bouquet, 15 years' experience).

We created ID side with the objective to give control back to internet users over commercial targeting online, empower them to set their privacy Choices in few clicks & **share their specific commercial interests seamlessly online**. Our goal is to foster an ethically & environmentally sustainable business model, which is an alternative to 24/7 digital tracking, facilitates qualitative exchanges between individuals and the Companies they trust/like and provides brand new user-controlled qualified leads.

The objective of ID side is also to help anyone effectively set their choices online (i.e. regarding Privacy, Safety, commercial preferences or Artificial Intelligence) and exercise their privacy rights seamlessly and automatically.

After years of Research and patenting our Tech, including in the US, we decided in 2024 to shift our main focus from at tool automatically sharing our reasonable expectations regarding "Cookie banners" (see our PoC on idside.eu / and the page idside.eu/cookies) to:

- Designing the second prototype for our "Personal Data Choices Management Platform" with the view of "sandboxing" it;
- launching a new "personal and private marketplace" so that individuals can easily set their commercial & algorithmic preferences (ID side app will be on Android in March).

On the long-run, ID side promotes an alternative and user-centric approach to online commercial targeting that we call the Light Web. In 2020, online commercial personalisation & ad targeting worked as follows:

- My data is collected online 24/7.
- It is sold so that ads get better directed to me.
- Companies sell such data without giving me control.

With ID side, and the Light Web model, individuals are empowered to take control over their data & ads displayed to them. They decide:

- How they want personal data to be collected online (our cookie banners extension).
- By Whom, When and How they want to be targeted (our personal & private marketplace).
- Which Companies they want to create a trusted relation with.

Our Research, Proof of Concepts (auto-filling of cookie banners) and latest prototypes (a personal and private marketplace) promote the **Light Web**, that is to say an alternative digital business model in which there are less data collected "in my back", I have more control on targeting & ads and companies unleash the benefits of an alternative **ethically & environmentally sustainable model**.

2. Why is it relevant for EDPB that ID side contribute to this Public consultation?

ID side team has a sound expertise in data protection and struggles to advance digital fundamental rights' state of the art tools -specifically with regards to individual-choices-automatic-sharing-online. Its "Personal Data Choices Management Platform" is designed to embed pseudonymisation techniques and empower internet users to share opt-out signals about any individual choice or right (regarding Privacy, AI, safety or any other right) but also their commercial preferences (into brands, products, sectors) in a de-identified way.

ID side team recognizes the significance of the consultation and the EDPB's role in advancing privacy rights globally and the understanding of Technology sate of play. We also express appreciation for the opportunity to provide feedback.

In this submission, ID side team would specifically like to provide feedback on the implementation of pseudonymisation in a practical case in the frame of individual automated Privacy signals (i.e. OOPS or GPC). At a moment in which the California 's Global Privacy Control is launched and the California Privacy Protection Agency (CPPA) enforces "*Opt-Out Preference Signals*" (OOPS) as "*a convenient and automated way for consumers to exercise their right to opt out of the sale and sharing of their personal data across all businesses they interact with online" ("Rather than submitting individual opt-out requests to each business, OOPS enables users to communicate their preferences in one seamless action*"), we believe that such use case could be relevant to the opinion in practice.

Importantly, ID side EU specific case enhances that having a strong "static" pseudonymisation might not be enough to ensure the protection of individuals rights. Sometimes "dynamic pseudonymisation" is a must have to empower internet and substantially mitigate risks of reverse tracking or risks associated with fingerprinting.

We hope this contribution will provide a practical insight, for instance as a use case.

3. Dynamic Pseudonymisation: a strictly necessary technical requirement to properly de-identify individual Privacy signals automatically shared online

In ID side's system, user preferences for personal data processing are integrated into network communication. ID Side's technology allows internet users to broadcast their default privacy choices to information technology providers. Conversely, it also allows these information technology providers to ask specific internet users to grant them an exception to such default privacy choices.

In this use case, information technology providers need a way to **indirectly identify** a specific internet user, relying on strong pseudonymisation techniques. This is the context in which ID side's pseudonymisation methodology might be relevant to this consultation.

Pseudonymisation is a critical data protection technique that allows personal data to be processed in a manner that reduces the risks of re-identification. The method outlined in ID side WIPO-PCT claims presents an advanced system for communicating over a network while incorporating user-defined privacy preferences

The key pseudonymisation techniques include an encrypted identifier generation, decoupling personal data from network communication and setting a dynamic pseudonymisation system allowing a two-phase communication model to remain fully de-identified for online service providers.

NB: Due to IP considerations, ID side will not fully describe here-below our pseudonymisation technique but remains at EDPB's team disposal to provide targeted information.

1. Identified Privacy Risk addressed by Pseudonymisation

ID side's management system generates an encrypted identifier from the user's actual identifier (EID) and relies upon such pseudonymous identifier to make in API calls possible -allowing service providers online to know updated choices (a) to (g) of an individual for instance.

This approach creates a potential unexpected privacy risk: the pseudonymous identifier generated by ID side (EID) could be used by information technology providers to indirectly track users, somewhat like using a device address (e.g. reverse-tracking or using ID side identifier as part of its fingerprinting data processing).

2. ID side method to address such Risk: Decoupling Personal Data from Network Communication

ID Side counters this risk by using cryptographic mechanisms that make the pseudonymous identifier change continuously (for each online request), rendering it useless as a tracking tool.

These "privacy-preserving" encrypted pseudonymous identifiers replace the user's real identity in communication with remote systems.

The use of cryptographic transformations ensures that even if intercepted, the encrypted identifier does not reveal the original identity without decryption keys.

The online preferences management system stores user-defined preferences for personal data processing separately from the communication stream. This ensures that the user's personal data is not directly exposed to the remote system. The management system (ID side as a Personal Data Choices Management Platform) mediates requests and responses, ensuring controlled exposure of user information.

3. A Two-Phase Communication Model

A first communication is established based on user preferences stored in the management system. It is associated with an encrypted ID (EID).

A second communication occurs only if authorized by the management system.

This separation ensures that even if a remote system attempts to directly engage with the user, it must first go through ID side de-identifying management system.

The integration of pseudonymisation techniques in ID side method offers several advantages:

- **Enhanced Data Protection:** By encrypting user identifiers, the system prevents unauthorized entities from associating a user's identity with their actions. The separation of data storage and communication further reduces the risk of unauthorized access.
- **Secure Intermediary Role of Management System:** The management system acts as an intermediary, ensuring that only "anonymized data" is transmitted to remote services. This mitigates the risk of data breaches by preventing direct access to personal identifiers.
- **Implementation Considerations:** To effectively implement pseudonymisation in a real-world scenario, ID side must consider:
  1- **Cryptographic Standards:** Utilizing strong encryption algorithms to generate pseudonyms;

2- **Access Control Mechanisms:** Ensuring only authorized entities can decrypt or correlate pseudonymised data;
3- **Regulatory Compliance:** Aligning pseudonymisation processes with data protection laws and industry best practices;
4- **Scalability:** The pseudonymisation system must efficiently handle large volumes of user requests without performance degradation.

Conclusion

ID side's robust dynamic pseudonymisation framework enhances individuals' privacy in network communications. By leveraging request-based encrypted identifiers, structured communication phases, and a dedicated personal data management system, this approach ensures a high level of security and privacy control and forbids reverse-tracking online or "fingerprinting" practices.

Important note: Future implementations may integrate AI-driven anomaly detection to further strengthen user data protection in networked environments.

Our team would be happy to elaborate on such technique if useful.

Online consent: How can it be made valid in practice?

Online consent cannot be reduced to a binary choice. It relies on the scope of "what" should be consented to, "why" it matters specifically to individuals, "when," and more broadly, "how" it is provided. Far from being a black-or-white assessment, to be valid, consent should be legally offered, meaning in accordance with applicable fairness, transparency and accountability principles, under Recital 32 of the EU General Data Protection Regulation referring to a "*freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her.*"

Valid consent should be rooted in, or at least aligned with, the reasonable expectations of individuals, i.e., neither distorting nor constraining individuals' will to accept or reject one or several optional data processing options, on the top of strictly necessary ones.

[…]

What online consent should be

To reassess state-of-the-art consent (GDPR Recital 32), a Nov. 2024 article by Lorrie Cranor stresses that, globally, "notice and consent" does not work as is and should be given "*the legal and technical support it needs.*"

On the tech front, Cranor acknowledges the significant steps taken in the U.S. to empower individuals in practice, specifically providing them with appropriate tech tools. From the binary approach of "do not track" to the current Global Privacy Control in California "*which allows users to turn on a setting in their browser (or browser extension) that transmits a GPC signal to automatically opt out of websites selling or sharing their personal information*," she writes that "*for the first time privacy laws are requiring websites to respect automated privacy signals such as GPC*."

California law sets a new cornerstone for regulating valid consent, and a crucial landmark has been set to respect individuals' right to share automated privacy signals and have them automatically complied with. Since the adoption of the GPC and, after that, the settlement of the Sephora case in August 2022, such right factually and amicably entered into force.

Outside the EU, California/US internet users are the first to enjoy the right to an actionable automated privacy signal tool, giving them real opt-out control. The California Privacy Protection Agency is the DPA leading the charge on this tech-enabled consent framework and was created four years ago. Despite being a new DPA, it somehow sets the tone on how individual fundamental rights should be enforced in practice in a tech-enabled world.

On the legal front, the need is clearly identified too and announced by GPC model. It is all about giving individuals the chance to seamlessly share their reasonable expectations online and switch from consent collection tools such as consent management platforms to user-centric privacy choices tools, such as personal data choice management platforms.

[…]

In short, this "notice and consent 2.0" empowers everyone to take control over commercial processing and personalization online, as they proactively share automated privacy signals wherever they browse seamlessly.

So why don't we validly consent online yet?

The tech is there. Few legal provisions in California already made the point that, in a tightly limited timeframe, user-centric automated privacy control practices can be fostered and enforced. What we need now is a global, consistent and game-changing regulatory positioning. Cranor stressed, "*We need IoT devices that send and receive standardized privacy signals to well-designed user agents. We need enforceable penalties for data collectors that fail to honor automated signals or manipulate users into consenting to data practices. And, importantly, we need strong baseline privacy regulations [...]*".

Conspicuously, valid consent blockers, whatever they are, are not tech ones anymore. As of today, the main blocker to valid consent appears to be regulatory latency - the time for regulators to adapt regulation to state-of-the-art tech practices from CMPs to PDCMPs.

One year ago, the European Commission's Directorate-General for Communications Networks, Content and Technology recommended exploring signals from personal data choice management platforms under Draft Principle H of the cookie pledge. Indeed, for consent to be valid in practice, what most innovative and accountable companies need is support in showcasing the kinds of user-centric personal data choices management platforms have that could help them serve trusted personalized ads and services. In 2024 the Digital Advertising Alliance started exploring cross-services signal-based mechanisms that are similar to those designed in the EU and are subject to patent application.

So, let's move the discussion forward diligently and determine what a consistent tech-enabled consent mechanism should look like in the U.S., EU and globally

.