20 אוגוסט, 2026

EDPB Publishes New Guidance on Blockchain, Anonymisation and Web Scraping for AI

Client Updates

The European Data Protection Board (EDPB) has recently published a series of guidelines addressing new technologies and data protection measures. Alongside adopting the final version of its Guidelines 02/2025 on the processing of personal data through blockchain technologies (the "**Blockchain Guidelines**"), the EDPB has launched public consultations on two draft guidelines concerning anonymisation and the processing of personal data through web scraping for the development and deployment of generative AI models.

Together, these publications provide valuable insight into the EDPB's evolving interpretation of the General Data Protection Regulation ("**GDPR**") and reaffirm its continued focus on privacy protection through design, accountability and transparency.

Final Guidelines on Processing Personal Data Through Blockchain Technologies

The final version of the Blockchain Guidelines follows public consultation on the draft previously published by the EDPB, and largely preserves the approach set out in the draft. The Blockchain Guidelines reaffirm that blockchain is not inherently incompatible with the GDPR, but that certain properties of blockchain may present compliance challenges when personal data is being processed.

The Blockchain Guidelines emphasize that the mere deployment of blockchain technology does not, by itself, amount to a processing of personal data, nevertheless, it does affect the processing activity and its compliance with the GDPR. Accordingly, the risks to the rights and freedoms of data subjects must be evaluated in order to ensure that processing is done in a GDPR-compliant manner. The EDPB recommends that before implementing blockchain technologies, controllers assess whether the use of blockchain is necessary for the intended purpose. The EDPB observes that "blockchain technology reduces some risks and raises others", emphasizing that controllers should document the rationale for selecting a particular blockchain architecture and demonstrate why it is necessary and proportionate for the intended processing.

In keeping with the principles of data protection as enshrined in the GDPR, the EDPB also states that the principle of data minimization requires that only personal data that is necessary for the relevant processing purpose should be processed on-chain. Storing personal data directly on-chain should be avoided, and

controllers should prioritize the use of architectures that minimize the personal data that is on-chain. Where possible, permissioned blockchain models (i.e., blockchains where only authorized participants may read, write, or create blocks, as determined by a governing authority) should be used in order to facilitate accountability in data processing.

Overall, the EDPB makes it evident that blockchain's technical characteristics, including its immutability, do not relieve organizations of their obligations under the GDPR. Controllers using blockchain must ensure that the rights of data subjects can be effectively exercised and conduct a Data Protection Impact Assessment (DPIA) where blockchain-based processing is likely to result in a high risk to the rights and freedoms of natural persons.

In summary, the final Blockchain Guidelines do not represent a departure from the EDPB's original position but rather confirm a clear regulatory direction. Organizations considering the deployment of blockchain technology should evaluate GDPR compliance from the outset and integrate privacy requirements into the design of the solution. While the Blockchain Guidelines adopt a risk-based approach, they express a clear preference for permissioned governance models, off-chain storage of personal data and privacy-enhancing architectures that minimize identifiability.

Draft guidelines on anonymisation

The draft Guidelines 02/2026 on anonymisation (the "**Anonymisation Guidelines**") provide greater legal certainty on when data can be considered anonymous, and therefore no longer constituting personal data for the purposes of the GDPR. The Anonymisation Guidelines reflect recent rulings by the Court of Justice of the European Union (CJEU) and seek to establish a practical framework for assessing whether anonymisation has been effectively achieved.

Under the GDPR, data is considered anonymous if it does not relate to an identified or identifiable natural person. An individual is considered "identified or identifiable" if they can be distinguished from others in a specific context, using means that are reasonably likely to be used in a way that would make it possible to treat that individual differently. Determining whether or not the means are reasonably likely to be used is context-dependent, and therefore a determination that data is anonymous may differ depending on the circumstances and the party processing the personal data. The Anonymisation Guidelines emphasize that anonymisation is an **outcome**, rather than a specific technical measure.

The Anonymisation Guidelines propose a practical assessment framework to assist organizations that is based on three criteria: (1) whether an individual can be isolated from the dataset; (2) whether records can be linked to other information; and (3) whether information about an individual can be inferred. Where any of these risks remain, further analysis is required before the data can be regarded as anonymous.

The Anonymisation Guidelines distinguish between two approaches to applying the proposed framework, the contextual approach and the simplified approach. Both approaches are endorsed by the EDPB as valid methods for applying the framework, though they differ in status and function**.** Under the contextual approach, which reflects the GDPR legal standard, anonymity is assessed by reference to the capabilities and circumstances of the relevant entities, including whether they could access the data or other information through means reasonably likely to be used. For example, a hospital sharing de-identified patient records with a research institute would assess whether the institute - given its particular access to additional datasets, technical resources, and legal powers - could re-identify the individuals, rather than asking whether re-identification is theoretically possible by anyone. By contrast, the simplified approach is not a separate legal standard. Rather, it is a more conservative and operationally convenient method that disregards those entity-specific differences. In effect, it asks whether re-identification would be possible assuming that any relevant means exist and are accessible to someone - for example, if demographic data combined with certain medical information could theoretically enable re-identification, the simplified approach would treat the data as not anonymous, even if no relevant entity actually has access to that additional medical information. As a result, organizations may treat data as personal even where it would in fact be anonymous for the relevant entities. Even so, the simplified approach may still be useful because it is easier to apply, can provide greater confidence that data is truly anonymous, and can be used alongside the contextual approach to refine the analysis.

Draft guidelines on web scraping in the context of generative AI

As publicly available online information has become an increasingly important tool for AI development, the EDPB has also issued draft guidelines 03/2026 on web scraping in the context of generative AI (the "**Web Scraping Guidelines**"). The Web Scraping Guidelines clarify that where web scraping involves the collection and use of personal data, the GDPR applies throughout the entire processing lifecycle, including the collection, storage, organization and use of the data for training AI models. The Web Scraping Guidelines also make clear that the mere fact that personal data is publicly available online does not, by itself, permit its unrestricted collection or use for AI development.

The Web Scraping Guidelines emphasize that organizations engaging in web scraping must identify an appropriate legal basis for data processing, and pay particular attention to the principles of **purpose limitation** and **transparency**. It is also noted that any exemption from the obligation to inform individuals directly about web scraping must be assessed carefully on a case-by-case basis. Controllers should therefore not assume that direct notice may be omitted simply because providing it would be difficult or burdensome, but should carefully assess whether or not the relevant GDPR transparency exemptions apply to their activities.

The Web Scraping Guidelines offer various suggestions for controllers who are seeking to comply with the

principle of data minimization by ensuring that only information necessary for the intended purpose is being collected. Such measures include, for example, defining precise collection criteria, applying filters, and conducting a data mapping and inventory exercise (i.e., cataloging what personal data is likely to be collected and from which sources, in order to assess necessity and facilitate ongoing accuracy and compliance). The Web Scraping Guidelines also recommend steps to support the accuracy of scraped personal data, such as scraping only from reliable sources and timestamping and validating the data before incorporating it into AI models.

Both the Anonymisation Guidelines and the Web Scraping Guidelines are open for public consultation until October 30, 2026.

Should you have any questions regarding digital assets, blockchain activities, AI or related privacy considerations, our firm's specialists are available to provide expert guidance on privacy and regulatory compliance.

Key Contacts

Assaf Harel
Partner

Avital Haitovich
Partner

Rebecca Genis Shepetovsky
Partner

Reut Cohen
Associate