

Legal Watch – Data Protection June & July 2026



MISCELLANEOUS

EDPB, adoption of a common template for personal data breach notifications, June 10, 2026:

[edpb_template_2026_data_breach_notification_v1.0_en.docx](#)

To help companies and authorities comply with the GDPR (the European regulation on data protection), the European Data Protection Board (EDPB) has created a standard template for reporting data breaches.

What is the purpose of this template?

- It allows organizations to structure and simplify their declarations in the event of a data breach.
- It ensures that all necessary information (such as that required by Article 33 of the GDPR) is included.
- It facilitates the work of authorities, who can thus assess incidents more quickly. Thanks to predefined options and practical advice, this template saves time and helps avoid errors.

Impact for Imagine: This template will standardize and accelerate our crisis management procedure in the event of a data breach (e.g., loss of genomic files, ransomware). As a research structure managing sensitive health data, adopting this template will make it easier to comply with the strict 72-hour deadline imposed by Article 33 of the GDPR when notifying the CNIL.

CNIL, replay the webinar – Tracking pixels in emails: presentation of CNIL recommendations, June 15, 2026:

What does the CNIL mean by the term "tracking pixel"? How can we ensure that their use complies with regulations?

Following the publication of its [recommendations](#), the CNIL presents the applicable framework to help stakeholders better understand their obligations and ensure respect for individuals' rights.

[Link to the webinar](#)

[Q&A with the CNIL on the recommendations](#)

Impact for Imagine: If the Institute uses mailing tools (scientific newsletters, invitations to conferences, fundraising campaigns) integrating tracking pixels to measure open rates, immediate compliance is required. The use of these trackers without prior explicit consent is now clearly subject to sanctions. We must audit our email marketing tools, disable pixels by default, or implement a specific consent collection mechanism before

loading any third-party images, under penalty of reputational and financial risks. For databases already constituted, we must send an email to individuals to inform them and give them the opportunity to object.

CNIL, 23 new sanctions issued since January under the simplified procedure, July 06, 2026:

The CNIL has implemented a simplified procedure to sanction organizations that fail to comply with data protection rules. Unlike the standard procedure, here, a single person (the Chair or a member of the CNIL's restricted panel) decides on the sanction.

Limits of this procedure:

- The maximum fine amount is €20,000.
- The name of the sanctioned organization is not made public.

Good to know: All fines issued by the CNIL, whether concerning private companies or public administrations, are collected by the State and paid into the national budget.

Summary since January 2026: The CNIL has already issued 23 sanctions under this procedure, totaling €133,750 in fines. These sanctions mainly concern three types of infringements:

1. Abusive video surveillance of employees

Certain companies monitor their employees without respecting their privacy.

2. Non-compliance with cookie rules

Certain websites place advertising cookies (which require user consent) before the internet user has taken any action. Furthermore, it is often easier to accept all cookies than to refuse them. For example, a banner offers an "Accept All" button with a single click, but to refuse, one must:

- Click on "Customize"
- Then access an interface to disable each cookie one by one.

However, the law is clear: if a site allows accepting all cookies with one click, it must also allow refusing all of them with one click. Organizations that do not comply with this rule risk a fine.

3. Non-compliance with user rights and lack of cooperation with the CNIL

Out of the 23 sanctions, 8 concern non-compliance with access or erasure rights (for example, a company failing to respond to a request to delete personal data). Among these, 4 are linked to a lack of cooperation with the CNIL: certain

companies (including law firms or medical practices) did not respond to CNIL requests during the investigation.

Result: They received a fine, sometimes accompanied by an injunction (obligation to comply under penalty of paying an additional sum). Failing to respond to the CNIL is illegal.

EDPB, anonymization and scraping for generative AI, processing of data using blockchain technologies: adoption of the final version of the guidelines, July 7, 2026:

Understanding anonymous data :

The new EDPB guidelines clarify the concept of anonymous data, also taking into account the judgment of the Court of Justice of the European Union in [case C-413/23 P, EDPB/CRU, of September 4, 2025, and other CJEU rulings](#).

Data is anonymous if it does not relate to an identified or identifiable natural person. Whether this is the case may vary from one entity to another. Information may relate to a person due to its content, purpose, or effects. The existence of such a link may not be immediately obvious and might require further analysis.

A person is considered "identified or identifiable" if they can be distinguished from others in a specific context using means reasonably likely to be used in a way that allows them to be treated differently. Whether the means are reasonably likely to be used will depend on the perspective of the concerned entity and should be assessed in light of all objective factors. The guidelines also provide a practical framework for organizations to determine whether anonymization is successful.

The framework can be applied in two ways: either by evaluating the differences in capabilities between those who could identify the individual ("contextual approach") or, for the sake of simplicity, by disregarding these differences ("simplified approach"), if a data controller chooses to do so. The contextual approach reflects all the nuances of the legal standard regarding anonymization.

The simplified approach may go beyond the legal standard and may lead an anonymizing data controller to treat data as if it were not anonymous, even if it would effectively be so for certain concerned entities; however, this approach can be more practical and provide greater confidence that the data is truly anonymous.

The framework uses 3 criteria to test whether data is anonymous:

1. **No individualization of records:** It must not be possible to isolate an individual within the dataset.
2. **No correlation:** It must not be possible to link distinct datasets concerning the same individual.

3. **No inference:** It must not be possible to deduce, with near certainty, new information about an individual. If all three criteria are met, the data can be safely considered anonymous. If one of these criteria is not satisfied, further analysis should be conducted to determine if the data can be considered anonymous.

[Guidelines on anonymization \(PDF, in English\)](#)

Clarifying the implications of scraping for data protection in the development of AI :

Scraping (or web scraping) is an automated technique that allows for the massive collection of data on the internet, often without the knowledge of the data subjects. This practice can pose risks to personal data protection, especially when it fuels the development of artificial intelligence (AI). Generative AI (such as tools that create text, images, or voice) needs enormous quantities of data to function. However, caution is required: if this data contains personal information, the GDPR (the European regulation on data protection) applies.

What does the GDPR say about scraping? The European Data Protection Board (EDPB) has published guidelines to regulate this practice. Here are the key points:

1. A legal basis is mandatory

To scrape personal data, a valid reason (called a legal basis) is required, such as the consent of the individuals, for example.

2. Respecting GDPR principles

- **Purpose limitation:** Data must only be used for the stated objective (e.g., training an AI model).
- **Transparency:** Individuals must be informed that their data is being collected, unless exceptions apply.
- **Data minimization:** Collect only what is strictly necessary.
- **Accuracy:** Data must be reliable and up-to-date. The EDPB advises using reliable sources, recording the collection date, and verifying data before using it to train an AI.

3. Caution regarding sensitive data

The GDPR prohibits the processing of sensitive data (ethnic origin, health, political opinions, etc.). Possible exception: If the collection is incidental (unintentional) and strict measures are implemented to prevent their use, a derogation may be considered.

[Guidelines on scraping in the context of generative AI \(PDF, in English\)](#)

Guidelines on blockchains finalized after public consultation :

The guidelines help organizations using blockchain technologies to comply with the GDPR. The EDPB explains how blockchains work, evaluating the different possible architectures and their implications for the processing of personal data. In line with the objective of the [Helsinki Declaration](#) to strengthen dialogue with stakeholders, the committee also published a [report on the results of the specific public consultation](#), as well as a [version of the guidelines entitled "Track changes"](#).

Impact for Imagine:

- **Anonymization:** For our research data sharing or publication projects (criteria: no individualization, correlation, inference), the "simplified" approach suggested by the EDPB might encourage us to treat certain data as personal out of caution, impacting our "anonymized" research databases.
- **AI & Scraping:** If the Institute develops or uses generative AI models trained on web data, the legality of "scraping" is regulated. The use of health data (special category) accidentally collected during scraping remains prohibited except under very strict exceptions. We will need to rigorously document the legal basis (legitimate interest) and implement robust technical filters to exclude sensitive data before training.
- **Blockchain:** If the Institute explores blockchain for tracing patient consents, for example, these guidelines are crucial. They highlight the tension between blockchain immutability and the right to erasure (GDPR). Any new technological implementation must prioritize architectures where personal data is not stored "in clear" on the chain to remain compliant (e.g., storing identifying data off-chain with encryption on the blockchain).

CNIL, update of MR-001 and MR-003, what changes in 2026 – Replay the webinar, July 31, 2026:

The reference methodologies MR-001 and MR-003 are evolving. Incorporating needs expressed by stakeholders, the new MRs see their scope expanded: studies conducted abroad, information modalities (including digitally), nature of processed data, remote quality control, data recipients, etc. Regarding format, the MRs follow an updated plan and new documents have appeared: annexes dedicated to security and quality control, annotated MRs, compliance grids, etc.

[Replay the webinar.](#)

Impact for Imagine: The Reference Methodologies (MR-001 for internal processing, MR-003 for research) are expanding to explicitly include studies conducted abroad and digital information. Required action: Update our compliance commitments to cover our international collaborations (data transfers outside the EU) and validate that our patient consent/information forms (often digital today) meet the new standards.