DPO Newsletter
March 2025

IN BRIEF:

- **SANCTIONS–** 2024 review of the sanctions and corrective measures pronounced by the CNIL and sanction of a company for the excessive surveillance of its employees.
- **ARTIFICIAL INTELLIGENCE** – Clarification of the definition of AI systems by the European Commission and new recommendations from the CNIL to support responsible AI.
- **ANONYMIZATION/PSEUDONYMIZATION** – A search engine called to order by the CNIL and publication of guidelines by the European Data Protection Board.
- **RIGHT OF ACCESS** – European coordinated action identifies gaps in the implementation of the right of access.
- **TRANSFER OUTSIDE THE EUROPEAN UNION** – Publication of the CNIL guide on impact assessments of data transfers.

I. SANCTIONS TO REMEMBER

a. 2024 report on the CNIL's sanctions

In 2024, the Commission Nationale de l'Informatique et des Libertés ("**CNIL**") (France) issued **87 sanctions, including 69 under the simplified procedure** (here). This significant increase compared to 2023 (42 sanctions) and 2022 (21 sanctions) can be explained by the increasingly frequent use of the simplified procedure (almost three times more than in 2023).

As part of its ordinary procedure, the CNIL has sanctioned companies in particular for:

- **Commercial prospecting**: in particular for the failure to collect prior consent from individuals before sending commercial communications.
- **Health data processing**: in particular with regard to anonymisation (e.g. clarification of the qualification of data processed in health data warehouses).

As part of its simplified procedure, the CNIL has sanctioned (i) the failure to **cooperate** with the CNIL, (ii) the failure to comply with **the exercise of rights**, (iii) the failure to **minimise** data, (iv) the breach relating to the **security** of personal data, and (v) the breach of the regulations relating to **cookies**.

b. Excessive surveillance of employees: €40,000 fine for a company in the real estate sector

The CNIL, by deliberation SAN-2024-021 of December 19, 2024 (here), imposed a fine of **€40,000** on a company in the real estate sector for having set up excessive surveillance of its employees, by means of software for monitoring working time and employee performance and a continuous video surveillance system set up in employees' work and break areas. The CNIL has identified several shortcomings, in particular:

Failures	Details
Excessive surveillance	(i) The continuous recording of images and sounds of employees is contrary to the principle of data minimization (Article 5 of the GDPR); and (ii) There is no legal basis for implementing endpoint monitoring software (Article 6 of the GDPR).
Lack of information	Oral information on the implementation of the monitoring software does not meet the conditions of accessibility over time and, in the absence of a written

	record of it, its completeness is not established (Articles 12 and 13 of the GDPR).
Lack of security measures	The CNIL recalls the reinforced requirement for individualized access to administrator accounts, which have very extensive rights over personal data – here, several employees shared the same access to data from the surveillance software (Article 32 of the GDPR).
Lack of impact assessment (DPIA)	The systematic monitoring of employees at their workstations required the formalization of a DPIA (Article 35 of the GDPR).

II. TOWARDS RESPONSIBLE AI

a. Prohibited practices in artificial intelligence: the new guidelines of the European Commission

On 6 February 2025, the European Commission adopted guidelines on the definition of artificial intelligence ("**AI**") systems to help stakeholders identify whether a software system falls under AI. It should be noted that these guidelines do not address general-purpose AI models. The Commission has identified and clarified the 7 elements that make up the definition of 'AI system', introduced in Article 3(1) of Regulation (EU) 2024/1689 on AI:

Definition of the AI Act	Commission clarifications
Machine-based system	AI systems must be computationally driven and based on machine operations.
that is designed to operate at varying levels of autonomy	The deductive capacity of systems is key to ensuring their autonomy: an AI system must operate with a certain reasonable degree of **independence of action** (which excludes systems requiring full manual human involvement and intervention).
and that may exhibit adaptiveness after deployment	The condition of the system's self-learning capacity is **optional** and non-decisive.
and that, for explicit or implicit objectives	Explicit (encoded) or implicit (inferred from behavior or assumptions) objectives are internal and refer to the goals and results of the tasks to be performed. They are part of a broader notion of the "purpose" of the AI system, which corresponds to the context in which it is designed and how it must be operated.
infers, from the input it receives, how to generate outputs	This notion refers to the **building phase** of the AI system, and is therefore broader than just the phase of use of the system. The Commission distinguishes between AI systems and other forms of software that have only a limited capacity to analyse patterns and adjust autonomously their output.
such as predictions, content, recommendations, or decisions	AI systems are distinguished by their ability to generate nuanced results, leveraging complex models or expertly defined rules. The Commission details each of the terms of the definition.
that can influence physical or virtual environments.	AI systems are not passive but actively impact the environments in which they are deployed.

b. The CNIL's new recommendations for responsible AI

On February 7, 2025, the CNIL published new recommendations to support the development of responsible AI, in compliance with the GDPR (here). These relate both to the information of individuals and to the exercise of their rights:

- **Information**: **the data controller must inform individuals when their personal data is used to train an AI model**. This information can be adapted according to the risks to people and operational constraints and can therefore sometimes be limited to **general** information (when people cannot be contacted individually) **and/or global** information (when many sources are used, for example by indicating only categories of sources).
- **Rights of individuals**: the CNIL invites stakeholders to take into account the protection of privacy from the design stage of the model (e.g. anonymization strategy, non-disclosure of confidential data). The implementation of rights in the context of AI models can be difficult and **a refusal to exercise rights can sometimes be justified**. When these rights must be guaranteed, **the CNIL will take into account the reasonable solutions available and may adjust the conditions of delay**.

III. ANONYMIZATION AND PSEUDONYMIZATION UNDER DEBATE

a. The CNIL sends Qwant a reminder of its legal obligations

The CNIL has sent the search engine Qwant a **reminder of its legal obligations** (here). In the context of the display of contextual advertising, Qwant considered that it was transmitting to Microsoft essentially technical and anonymized data (e.g. truncated or hashed IP address). Following two inspections and exchanges with its European counterparts, the CNIL considered that the data transferred is pseudonymised and not anonymised.

It chose to issue a reminder of the company's legal obligations rather than a sanction due to: (i) the low level of **intrusiveness** of the search engine, (ii) the numerous **technical measures** deployed to reduce the risk of re-identification, (iii) the **unintentional nature** of the breach, resulting from an initial analysis error, (iv) the **rapid** modification its privacy policy, and (v) its **good faith and cooperation** throughout the procedure.

b. The new EDPS Guidelines on pseudonymisation

On 16 January 2025, the European Data Protection Board (EDPB) adopted new guidelines 01/2025 on pseudonymisation, which are subject to public consultation until 14 March 2025.

Pseudonymisation means that personal data is no longer attributed to a data subject without additional information (Article 4(5) GDPR). **Pseudonymised data is personal data because there is a risk of re-identification of the data subjects.**

The EDPB states that pseudonymisation can (i) **facilitate the use of the legal basis of legitimate interest**, provided that all other requirements of the GDPR are met, (ii) ensure **compatibility with the original purpose** in the context of further processing, and (iii) help organisations comply with obligations relating to the principles of the GDPR, protection by design and by default, and security.

The EDPB is also analysing a set of robust technical measures to prevent unauthorised re-identification. Recommended techniques include **hashing with a secret key or salt, separation of information for attribution, and strict access control**.

It will be pointed out that these guidelines are to be read in the light of Case C-413/23 pending before the Court of Justice of the European Union between the European Data Protection Supervisor and the Single Resolution Board (SRB). In this case, pseudonymised data was transferred by the SRB to Deloitte for the purposes of an analysis mission. In his Opinion of 6 February 2025, the Advocate General asks the Court to rule on whether the recipient of pseudonymised data who does not have reasonable means to re-identify the data subjects could be considered not to be processing personal data insofar as the risk of identification is 'non-existent or insignificant'.

IV. SPOTLIGHT ON THE RIGHT OF ACCESS

The CNIL and the European Data Protection Supervisor participated in a coordinated action of the European Data Protection Board in order to evaluate the implementation of the right of access to personal data.

During 2024, the CNIL inspected public and private bodies, chosen on the basis of complaints received, and issued several reminders of legal obligations. She notes that the organizational measures implemented by these organizations to process right-of-access requests are sometimes insufficient/unsatisfactory. Organizations should both (i) **provide information about the processing,** (ii) **include a copy of the data processed**, and (iii) should not systematically exclude certain processing or categories of personal data from their responses.

The EDPS has monitored the processing of requests for the right of access by the EU institutions, bodies, offices and agencies and has highlighted in his report of 16 January 2025 : (i) the low volume of requests, (ii) the decentralisation of the management of requests, (iii) the fact that it is difficult to distinguish between access requests and other types of requests, (iv) the excessive processing of data caused by the verification of the identity of applicants, (v) the difficulty of reconciling the protection of rights and freedoms and respect for the right of access of individuals. Controllers and processors are invited by the EDPS to refer to Guideline 01/2022 on the right of access of data subjects.

V. IMPACT ANALYSIS OF DATA TRANSFERS

On January 31, 2025, the CNIL published the final version of its guide on the Impact Assessment of Data Transfers (AITD) (here) to help data exporters assess the level of protection in destination countries located outside the European Economic Area and the need to put in place additional safeguards. This analysis is necessary when the transfer is based on a tool of Article 46 of the GDPR (standard contractual clauses, binding corporate rules, etc.): the destination country does not benefit from an adequacy decision and the transfer is not carried out on the basis of a derogation from Article 49 of the GDPR.

The guide proposes a six-step methodology:

1) Identify the data concerned and the actors involved;
2) Choose the appropriate transfer tool;
3) Analyze risks related to the laws and practices of the third country;
4) Determine and apply additional measures (e.g. encryption or anonymization);
5) Implement these additional measures;
6) Reassess the compliance of the transfer at appropriate intervals.

This publication follows a public consultation that allowed the CNIL to adapt its guide to the practical realities of companies, and to modify it in order to take into account the latest opinions of the European Data Protection Board.