King & Spalding

Client Alert

Data, Privacy and Security

MAY 16, 2025

For more information, contact:

Charly Helleputte
+32 2 898 0237
chelleputte@kslaw.com

Andrea Otaola
+32 2 898 0240
aotaola@kslaw.com

King & Spalding

Brussels
Bastion Tower
5 Place du Champ de Mars
Brussels 1050
Tel: +32 2 898 0200

New Security Measures for Large Databases: When a DPA's Directives Set Standards

In response to a record year of personal data breaches in 2024, affecting millions of individuals, the French data protection authority (CNIL) has published a set of security directives for operators of large databases. While EDPB and domestic guidelines are often criticized for being vague in their guidelines, the CNIL is taking a very different approach and sets standards that have wide ranging effects.

Large databases are systems that facilitate the processing and access of a specific set of personal data for several million individuals (comprising all the components, networks, and applications involved in such processing).

WHY ARE ADDITIONAL SAFEGUARDS NEEDED?

Existing GDPR provisions (notably articles 5(1)(f) and 32) call for appropriate security requirements. The CNIL believes that additional, specific safeguards are needed in the context of large databases.

The CNIL emphasizes that, given their scale, large databases pose heightened risks: a single vulnerability can expose large populations and facilitate cascading attacks.

ESSENTIAL MEASURES FOR LARGE DATABASES

1. Mandatory Multi-Factor Authentication (MFA)

Noting that many 2024 breaches involved compromised credentials, the CNIL emphasizes MFA as a baseline requirement for all external access to large-scale personal data systems. Adding a second authentication is an effective way to significantly reduce the risk of unauthorized access following an identity theft.

In this regard, the CNIL quotes both its recent guidance "recommendation relating to multi-factor authentication", as well as one

from ANSSI's "recommendations relating to multi-factor authentication and passwords".

MFA has to be deployed after carrying out a risk analysis taking into account threats in connection with the different means of accessing the data and favoring the use of authentication based on knowledge (i.e. password) and possession (i.e. connected phone).

This type of measure must be part of a broader identity and access management policy that each organization must implement and maintain, based on user profiles.

2. Log, Analyze and Set Limits on Data Flows Passing Through the Information System

To prevent large-scale unauthorized exports, the CNIL calls for technical controls such as implementing appropriate logging and establishing download limits per session.

In particular, the authority recommends the following measures for both data controllers and processors, as included in its recommendation relating to logging and ANSSI's guidelines of the architecture of a logging system:

- Implement a logging architecture to ensure traceability of access and actions of the various users authorized to access information systems, for a period of between six months and one year. A good practice is to log access (to applications, APIs, the system, the network) separately from the main system ("log sink").
- Implement the logging system in a targeted manner to enable the detection of potentially suspicious activity as soon as possible, prioritizing monitoring on sensitive areas rather than accumulating unnecessary logs.
- Determine which events to log based on context and devices to detect abnormal data flows, allow only authorized flows, track successful and rejected logins, control data flow, and identify configuration flaws or SQL injections.

3. User Engagement and Security Awareness

Organizations are urged to implement targeted and recurring security training for all relevant stakeholders, including internal teams and subcontractors.

Be ready to be asked to demonstrate those took place in the course of any CNIL' investigations or audits. Failure to provide effective, documented training may be interpreted as noncompliance with security obligations.

4. Enhanced Oversight of Processors

Given the frequent role of third-party service providers in breach incidents, especially in cloud environments, the CNIL expects data controllers to undertake robust due diligence, contractual controls, and ongoing audits across their entire subcontracting chain. The authority highlights the importance of the subcontractor benefiting from the same level of enhanced security as the data controller.

This includes the obligation for data controllers to require subcontractors to have their Information Systems Security Policy and proof of their information security certifications in the contract. In addition, it is also essential for data controllers to ensure that the subcontractor's security measures are cutting-edge and thoroughly checked during regular audits or inspections. Even if the CNIL doesn't state it expressly, sound contracting strategies that will include audit rights, are also to be developed.

EXPECT AUDITS IN 2026, GET READY IN 2025

It is important to note that the CNIL refers to these measures not as recommendations or best practices, but as directives, a deliberate choice underscoring their binding character.

While implementation may require significant investment, the risks of non-compliance, both in terms of data exposure and regulatory sanctions, are considerable.

The CNIL has specifically announced that compliance with MFA requirements will be a priority audit focus from 2026 onward.

Large databases are often not geographically confined to a single member state. Therefore, the CNIL's guidance is valuable beyond France. Same for smaller players that do not fall per se within the scope of the recommendations. Indeed, the additional requirements are setting the tone of best practices one might be benchmarked against. It is time to revisit current practices, gap assess them and deploy additional measures, as appropriate.
