BCLP. Client Intelligent

Insights

CNIL PUBLISHES ‘AI HOW-TO SHEETS’ ON ALIGNING ARTIFICIAL INTELLIGENCE SYSTEMS WITH GDPR

Oct 25, 2023

SUMMARY

A few days ago, the French Data Protection Authority (CNIL) published its first draft guidelines for the use of AI systems in the form of "AI How-To Sheets" with the aim to “help professionals reconcile innovation with respect of people’s rights”.

These guidelines aim to guide industry stakeholders on the alignment of artificial intelligence with the General Data Protection Regulation (GDPR). In particular, it sheds light on how AI databases can adhere to principles of data purpose, minimisation and retention.

Following a public consultation period that will end on 16 November 2023, the CNIL is scheduled to release the finalised guidelines in early 2024.

SCOPE OF THE AI HOW-TO SHEETS

These how-to sheets are primarily aimed at machine-learning AI systems (also known as statistical or stochastic systems, as well as knowledge-based or deterministic systems). The guidelines pertain only to the AI systems' development phase, excluding the deployment phase.

This development phase can be further segmented into three stages: (i) AI system design, (ii) database creation through data collection and pre-processing, and (iii) the system's learning and training.

Below are the key takeaways of each how-to sheet published by the CNIL.

SHEET 1 – DETERMINING THE APPLICABLE LEGAL REGIME

The CNIL highlights that, depending on when the operation use of the AI system is defined, the legal framework applicable during the development of an AI system might differ or overlap with the

framework applied during its deployment. Data processing operations during the development are generally under the GDPR's scope.

SHEET 2 - DEFINING A PURPOSE

Before collecting or processing personal data, it is imperative to clearly define the purpose of such processing. The CNIL underscores that this purpose should be explicit, legitimate, and easily understandable to the concerned individuals. However, if the purpose for deploying the AI system has not been clearly defined, or if it differs from its initial objectives during the development phase, it is still deemed precise enough if it specifies both the kind of AI system being developed (like generative AI or a language model) and its anticipated technical functionalities and capabilities. As such, the simple aim of "developing a generative AI model" is not considered compliant.

SHEET 3 - DETERMINING THE LEGAL QUALIFICATION OF AI SYSTEM PROVIDERS

The CNIL's information sheets provide clarity on the various roles in the AI development process, such as the data controller, joint controller, and data processor, and their respective responsibilities.

SHEET 4 - ENSURING LAWFUL DATA PROCESSING

AI entities must determine the lawful basis under the GDPR for processing data, whether it is through obtaining explicit consent from the user, processing data based on legitimate interest, public interest, or due to contractual obligations.

SHEET 5 - CARRYING OUT A DATA PROTECTION IMPACT ASSESSMENT (DPIA) WHEN NECESSARY

Given the potential risks associated with AI systems, such as automated discrimination, errors in content generation, and possible attacks on AI systems, the CNIL elaborates on the importance of conducting a DPIA to ensure data protection.

It is important to note that the CNIL does not consider the use of AI systems as an inherently innovative use or the application of a new technological or organisation solution. As such, not all processing through the use of AI systems will meet this criterion.

Similarly, the CNIL makes clear that whilst the development of an AI system often relied on processing a large amount of data, this does not necessarily fall within the scope of large-scale processing. It is necessary to determine whether the development involves a large number of data subjects.

The CNIL highlights key risks linked with AI systems to consider during a DPIA. These include:

- misuse of training data, especially during data breaches

- AI-driven discrimination affecting system performance for certain groups
- potential for generating inaccurate content about individuals, impacting their reputation
- confirmation biases in automated decision-making, particularly if there is a lack of transparency or if decisions cannot be challenged
- users losing control of their data, often collected in large-scale operations for AI training, notably through web scraping (as explored earlier)
- vulnerabilities to specific AI attacks such as data poisoning, backdoor insertion or model inversion
- confidentiality risks surrounding data that may be retrieved through AI systems.

SHEET 6 – TAKING DATA PROTECTION INTO ACCOUNT IN THE SYSTEM DESIGN CHOICES

Data controllers are responsible for ensuring compliance with data protection principles including:

- establishing the primary goal of the system
- determining the system's technical architecture
- identifying data sources and selectively using only the data that is necessary for the intended purpose (adhering to the principle of data minimisation – ensuring data collected and used is relevant, suitable and limited to its intended purpose)
- evaluating and confirming previous decision, potentially in consultation with an ethics committee
- designing the technical architecture
- ensuring the selection of the data sources and the use of data is strictly necessary.

SHEET 7- TAKING DATA PROTECTION INTO ACCOUNT IN DATA COLLECTION AND MANAGEMENT

In the last practical information sheet, the CNIL summarises the main 'good practices' and how to apply data protection principles to the management of learning data. These include:

- aligning data collection with GDPR principles, in particular during 'web scraping'
- rectifying errors, addressing missing values and discarding duplicates of irrelevant data

- implementing measures to integrate the principles of personal data protection (or ‘privacy by design’)
- monitoring the data collected and the purposes for which it was collected to ensure it is accurate, relevant, adequate and limited
- setting a clear data retention period

implementing appropriate technical and organisational measures to guarantee data security.

THE BENEFITS OF THE AI HOW-TO SHEETS TO AI COMPANIES AND AI CREATORS

As AI is an emergent technology lacking a distinct legal status, keeping updated with new regulatory frameworks is crucial. The information sheets published by the CNIL provide a robust foundation for European AI companies, enhancing their comprehension of personal data processing's legal intricacies.

However, the CNIL cautions that these information sheets are a mere starting point, designed to assist professionals in reconciling innovation with individuals' rights. There remain many other themes and questions that demand attention for a comprehensive legal framework around personal data processing – both during the upstream development and downstream deployment phases.

BCLP will be following the publication of the final practical information sheets to offer its clients informed advice on adapting to the CNIL's recommendations during AI development.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
