Global Data and Cyber Handbook - France

Regulators, Enforcement Priorities and Penalties

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: January 2025*

The [French Data Protection Authority](https://www.cnil.fr/en/home) (*Commission nationale de l'informatique et des libertés*, "**CNIL**") is an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data. Under the SREN Law, the CNIL is also competent for “data altruism”.

In regards with non-personal data, the SREN Law has designated the French regulatory authority for electronic communications, post and press distribution (the "**ARCEP**") as the regulator in charge of "data intermediaries" under the Data Governance Act.

Also, the National Agency for the Security of Information Systems ("[**ANSSI**](https://www.ssi.gouv.fr/en/)") is the national authority responsible for supporting and securing the development of digital technology. As such, ANSSI plays a major role in cybersecurity, and provides services for monitoring, detecting, alerting, and reacting to computer attacks and ensuring the security of citizens' data.

# How active is each of the regulator(s)?

*Last review date: January 2025*

CNIL : ☒ Very active

ANSSI : ☒ Moderately active

# What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: January 2025*

 The CNIL has published its annual control plan for 2024 focusing on four main topics, available [here](https://www.cnil.fr/fr/les-controles-de-la-cnil-en-2024-donnees-des-mineurs-jeux-olympiques-droit-dacces-et-tickets-de):

**Data collection for the Olympic and Paralympic Games** : in the context of this international sports competition, the CNIL was mobilized before and during the games to ensure that data subjects' privacy was respected.

**Minors' data collected online** : the CNIL mainly focused on checking whether websites and applications popular among minors are compliant with the obligation to verify the age online.

**Loyalty programs and dematerialized receipts :** the focus was on loyalty programs by offered to customers by supermarkets, and more importantly since the dematerialization of sales receipts (instituted by Law No. 2020-105 of February 10, 2020 on the fight against waste and the circular economy – link [here](https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041553759/)).

The CNIL should release its annual control plan for 2025 in spring 2025.

Please note that, based on the available resources published as of December 2024, 75 % of CNIL's inspections flow from complaints and/or data breaches notifications. As a result, CNIL's annual control plan benefits only from 25% of its available resources.

The CNIL has also published its strategic plan for 2022/2024 focusing on three priority axes, available [here](https://www.cnil.fr/en/cnil-publishes-its-2022-2024-strategic-plan):

Promoting the control and respect of data subjects' rights;

Promoting the GDPR as a trusted asset for organizations;

Prioritizing targeted regulatory actions on topics with high privacy stakes such as (1) augmented cameras and their uses on the basis of the CNIL's upcoming guidelines on "*smart or augmented cameras in public spaces"*, (2) data transfers as part of cloud computing and (3) collection of personal data by smartphones' applications.

The Digital Innovation Lab of the CNIL ("**LINC**") has published its research strategy plan for 2022/2023 focusing on four main subjects:

The impact of data protection on the protection of the environment

The new economies of data (in particular the topic of data brokers)

The practices and perceptions of the data subjects regarding the means available to protect their privacy and the exercise of their rights

Capturing data

The LINC has not published a new strategic plan for 2024.

# What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: January 2025*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒         Staying the same

Class actions/group actions under data or cyber regulation are:

☒         Rare

# What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: January 2025*

There are:

☒        administrative remedies / civil penalties applied by regulators and law enforcement

Unless the data controller is the State, the CNIL may impose the following administrative fines:

In an amount of up to EUR 10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In the cases referred to in Article 83(5) and (6) GDPR, in an amount of up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In the case where the sanction proceeding is simplified (i.e., subject to article 22-1 of the Data Protection Act ), the amount is up to EUR 20,000

☒        criminal penalties from regulators and law enforcement

Pursuant to article 40 of the Data Protection Act, some offenses against Data Protection Act provisions are provided for and punished by articles 226-16 to 226-24 of the Criminal Code. The fines described below for alleged breaches of articles 226-16 to 226-24 of the French Penal Code are multiplied by 5 ("amende au quintuple") under article 131-8 of the same Code if the perpetrator is a legal entity.

They include:

Processing personal data, including through negligence, or having it processed by a third party without compliance with formalities to take prior to their implementation, as provided for by law, is punishable by five years' imprisonment and a fine of EUR 300,000.

Processing personal data including information about the registration numbers of individuals in the national register of identification of natural persons, without authorization, is punishable by five years' imprisonment and a fine of EUR 300,000.

Processing personal data or having it processed without implementing measures prescribed in articles 24, 25, 30 and 32 of the GDPR (i.e., responsibility of the controller, data protection by design and by default, records of processing activities, security of processing) is punishable by five years' imprisonment and a fine of EUR 300,000.

Failure by an electronic communications service provider or controller or processor to notify a breach of personal data to the CNIL, or the data subject (or the controller in the situation of a processor) is punishable by five years' imprisonment and a fine of EUR 300,000.

Collecting personal data by fraudulent, unfair, or unlawful means is punishable by five years' imprisonment and a fine of EUR 300,000.

Processing personal data concerning a natural person despite that person's opposition, where such processing is for the purpose of prospecting, in particular for commercial purposes, or where such opposition is based on legitimate grounds, is punishable by five years' imprisonment and a fine of EUR 300,000.

Data retention (except in cases provided for by law), without the express consent of the data subject, of sensitive personal data is punishable by five years' imprisonment and a fine of EUR 300,000. The same penalties apply to non-automated processing of personal data, which implementation is not limited to the exercise of exclusively personal activities.

Processing personal data for the purpose of health research is punishable by five years' imprisonment and a fine of EUR 300,000: when no information has been provided to the data subject about transfers, right of access, rectification and opposition, the nature of the data transmitted and the recipients of such data; when notwithstanding the opposition of the data subject or, where provided by law, in the absence of the person's informed and express consent, or in the case of a deceased person, notwithstanding the refusal expressed by the latter during their lifetime.

Retaining personal data beyond the period provided for by law or regulation is punishable by five years' imprisonment and a fine of EUR 300,000, unless such retention is carried out for historical, statistical, or scientific purposes under the conditions provided for by law.

Misuse of defined purposes is punishable by five years' imprisonment and a fine of EUR 300,000.

Unauthorized disclosure of data which would have the effect of violating the consideration of the data subject or their private life, or of causing damage to their privacy, shall be punishable by five years' imprisonment and a fine of EUR 300,000, or a fine of EUR 100,000 where it has been committed through negligence or carelessness. Prosecution can only be carried out upon a complaint from the victim, their legal representative, or successors in title.

Transfers of personal data in violation of Chapter V of the GDPR is punishable by five years' imprisonment and a fine of EUR 300,000.

It is punishable by one year's imprisonment and a fine of EUR 15,000 to obstruct actions of the CNIL, either by opposing the performance of the tasks entrusted to its members or to authorized agents when the visit has been authorized by the judge; either by refusing to communicate to its members or to the agents authorized the information and documents relevant to their mission, or by concealing or removing such documents or information; by communicating information that does not conform to the content of the recordings as it was at the time the request was made or that does not present such content in a directly accessible form.

Pursuant to article 226-23 of the Criminal Code, in the cases provided for above (i.e., as set out in Articles 226-16 to 226-22-2), the erasure of all or part of the personal data processed in respect of which the offense was committed may be ordered. The members and agents of the National Commission for Informatics and Liberties are entitled to note the deletion of these data.

Finally, legal persons found criminally liable, under the conditions provided for in article 121-2, for offenses defined in the aforementioned situations, shall be liable to the penalties provided for in articles 131-39, 2° to 5° and 7° to 9° of the Criminal Code.

☒        private remedies

Individuals may, for example:

file complaints with the CNIL (article 11 of the Data Protection Act)

claim damages for material or non-material damages (article 43 Ter of the Data Protection Act)

More precisely, in relation to judicial proceedings, the current group action provided for in article 43 Ter of the Data Protection Act can only terminate a violation of the Data Protection Act and cannot compensate data subjects for damages resulting from such a violation.

Pursuant to article 43 quarter, any person may mandate/appoint an association or organization referred to in article 43 Ter to exercise on his or her behalf the rights provided for in Articles 77 to 79 and 82 of the GDPR (i.e., right to lodge a complaint with a supervisory authority, right to an effective judicial remedy against a supervisory authority, a controller or a processor, and right to compensation and liability). It may also mandate them to act before the CNIL, against the latter before a judge or against the controller or their processor before a court.

# If data subjects have private remedies, what form can these remedies take?

*Last review date: January 2025*

☒        individual personal actions

☒        representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.