



# Cybersecurity

GDPR: the best prevention  
against cyber risks

## » GDPR, A CYBERSECURITY INSTRUMENT

### Information security, an obligation since 1978, a framework reinforced with the GDPR

Security is one of the fundamental principles of the Data Protection Act. A lack of security in the processing of personal data entails the risk that data could be retrieved by a malicious third party and used against the data subjects.

The GDPR increased the requirements for personal data security. It has confirmed the role of data protection authorities in supporting all companies and administrations in this particular area.

#### SECURITY OBLIGATIONS UNDER THE GDPR

**Implement technical and organisational measures to secure data**

**Keep a record of data breaches**

**Conduct a Privacy Impact Assessment (PIA)**

> For certain sensitive processing operations

**Notify the CNIL of a data breach**

> If there is a risk to individuals

**Inform individuals of a data breach**

> If there is a high risk to individuals

The GDPR is the only text to impose specific cybersecurity obligations on all organisations, regardless of size and sector, and which are subject to the investigatory and enforcement powers of an administrative authority such as the CNIL.

In the event  
of non-  
compliance

Administrative fine  
of 20 million euros  
or 4% of turnover

The CNIL supports administrations and companies in mainstreaming computer security.

The security principle, enshrined in the law for more than 40 years, has been strengthened by the GDPR and supplemented by new obligations and tools such as notification of data breaches, data protection impact assessment, codes of conduct or certification.

## IN FIGURES

**5,037**  
notifications

of data breaches in 2021.  
**+79%** vs. 2020.

over **2,150**  
notifications

of data breaches resulting  
from a **ransomware attack**  
received in 2021, i.e.  
**43%** of the total volume.

**1/2**  
of the sanctions

issued by the CNIL in 2021  
relate to non-compliance  
with the security obligation.



FOCUS

### What is a Privacy Impact Assessment (PIA)?

The PIA is a tool used to build a processing that complies with the GDPR and respects privacy. It applies when the processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects. When residual risks remain high, the GDPR provides that a data controller must consult with its supervisory authority (the CNIL in France) prior to implementing the processing operation. If it proves impossible to sufficiently reduce the risks at the end of this exchange phase, then the supervisory authority may issue an opinion stating that the planned processing is in breach of the GDPR.

Find out more

[www.cnil.fr/en/privacy-impact-assessment-pia](http://www.cnil.fr/en/privacy-impact-assessment-pia)

# PERSONAL DATA BREACH NOTIFICATIONS

## What is a data breach?

According to the GDPR, a personal data breach is “a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.”

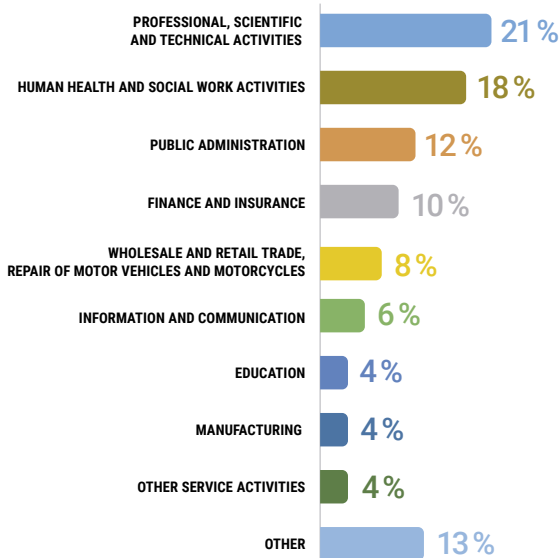
This means any security incident, whether malicious or not, and whether intentional or not, that results in the **integrity**, the **confidentiality** or the **availability** of personal data being compromised.

Some examples:

- ▶ **accidental deletion of medical data held by a health institution and not otherwise backed up;**
- ▶ **loss of an unencrypted USB key containing a copy of a company’s customer database;**
- ▶ **malicious connection to a school database and modification of pupil results obtained.**

**+79% increase in the number of data breaches notified to CNIL in 2021 compared to the previous year. On average, almost 14 notifications received per day.**

## Sectors most affected (2021 figures):



## Nature and causes of notified data breaches

**80%** of the data breach notifications received by the CNIL relate to a **loss of confidentiality**, i.e. penetration by a third party who could gain knowledge of the data or even copy it.

Although the GDPR considers that a personal data breach can also result from a security incident leading to a loss of integrity or availability, statistics show that this type of data breach is seldom notified by data controllers.

### THE GDPR REQUIRES DATA CONTROLLERS TO:

- > document personal data breaches internally;
- > notify the CNIL within 72 hours when the breach presents a risk to the rights and freedoms of individuals;
- > inform the data subjects where this risk is high.

Although marginal compared to notifications of confidentiality breaches, the CNIL observed a **clear increase in notifications related to a loss of integrity (data modified illegitimately) and availability (data inaccessible for a certain period of time)**. This is due in particular to the increasing number of breaches caused by **ransomware attacks**.

Further, the obligation to notify the supervisory authority of a data breach relates to breaches of accidental or unlawful origin. The majority of notifications received by the CNIL in 2021 concern data breaches originating from a malicious external act (hacking, theft of physical media or fake technical support scams).

## HACKING IN 2021

- **59%** of all notifications to the CNIL, i.e. **3,000** notifications. **(+128% vs. 2020)**.
- **43%** of notifications relate to a ransomware attack.

## USEFUL RESOURCES

- ▶ Technologies to protect information assets and protect data subjects from breaches of their personal data: [www.cnil.fr/fr/cybersecurite](http://www.cnil.fr/fr/cybersecurite) (in French only)
- ▶ Computer emergency response team – to be checked daily: [www.cert.ssi.gouv.fr](http://www.cert.ssi.gouv.fr) (in French only)
- ▶ ANSSI Agence nationale de la sécurité des systèmes d’information (French National Cyber Security Agency): [www.ssi.gouv.fr/en](http://www.ssi.gouv.fr/en)
- ▶ Assistance and prevention on digital security: [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr) (in French only)

## › THE ROLE OF THE CNIL IN CYBERSECURITY

In addition to being a legal obligation, security of personal data is a major issue for all public and private organisations, as well as for all individuals. The CNIL fully plays its role in cybersecurity, acting primarily around four areas:



### Raising awareness among the general public

In order to raise public awareness on the issues of personal data security in everyday use, the CNIL has developed various resources. It has published a guide on *"How to protect my data"*, and provides a number of fact sheets on its website, including:

- › Phishing: detecting a malicious message
- › Preventing, spotting and reacting to the hacking of your social accounts
- › How to react to a webcam blackmail
- › Four ways to better protect your identity online
- › How to react to identity theft
- › Ten tips to stay clean on the web
- › The CNIL's advice for a good password
- › Private browsing to limit the risk of hacking in your online accounts

The CNIL is also setting up partnerships with relays within civil society and companies.

### Providing guidance to professionals

In implementing an effective cybersecurity policy, all steps are essential. In order to provide professionals with the best possible guidance, the CNIL shares its expertise through a number of resources, including:

- › a recommendation on passwords, to be updated soon;
- › a recommendation on event logging;
- › a general guide to data security together with a checklist;
- › fact sheets on secure websites and information systems;
- › regular publications on examples of frequent data breaches (ransomware, CEO scams, attacks on messaging, attacks on cloud configuration faults, credential stuffing, etc.)

In addition to this general advice, which is applicable in most cases, the CNIL also publishes reminders and best practices for different sectors of activity in its various guides (VSEs/SMEs, associations, local authorities, etc.). The issue of data security also plays an important role in projects that benefit from intensive support from the CNIL as part of its "sandbox" scheme, which launched in 2021 with the theme of digital health, and this year focuses on EdTech.

## Specific support for VSEs/ SMEs

The CNIL makes various tools available on its website to support VSEs/SMEs, such as the guide to GDPR awareness co-edited with Bpifrance, a GDPR checklist, benchmarks, the guide to data retention periods, a simplified template for processing records and also fact sheets. To maximise its impact, the CNIL has set up a strategy known as "network heads", which is essential for indirectly reaching all players via associations or professional networks and organisations. The latter also produce, with the assistance of the CNIL, practical guides and assessment tools based on the specific activities of their members.

## Awareness within organisations is still lacking

All organisations are now affected by attacks, regardless of their size or sector.

The CNIL has noted increased awareness of cybersecurity issues within organisations, with managers, data protection managers, risk and security managers and IT departments. However, there is still no data protection without security.

Although this improvement has resulted in better anticipation in IT protection, it is not yet fully implemented. In particular, medium-sized organisations, which are often impacted by the increasing number of ransomware attacks hitting all companies and sectors.

The CNIL has also noted shortcomings linked to the failure to deploy adequate security solutions. Breaches notified. The implementation of these solutions must become systematic.

## Systematic checks and and deterrent sanctions

Information security is systematically covered in the 300 formal inspection procedures conducted by the CNIL each year. For instance, compliance with basic principles is checked (passwords, database and network security, etc.), as well as the existence of a breach register, a new obligation under the GDPR.

### The most frequent infringements:

- ▶ data freely accessible by modifying a URL (lack of authentication, predictable URL), e.g. simply modifying a number in the address bar enables access to other people's documents;
- ▶ a password policy that does not comply with the CNIL's password recommendation;
- ▶ the transmission of passwords in clear text, for example when creating an online account;
- ▶ the transmission of data over unencrypted channels (HTTP), for example in the case of an online form used to send personal data;
- ▶ the absence of automatic locking of workstation sessions, enabling a third party to access an information system containing personal data;
- ▶ insufficient testing to verify the absence of vulnerabilities before rolling out a new system. This is the case when an organisation develops a new tool (application, website, form) that processes personal data, without providing for a test phase to identify possible vulnerabilities.

## Participation in the cyber ecosystem

The CNIL has developed numerous partnerships with key players in cybersecurity, in particular with the French National Cyber Security Agency (ANSSI).

Awareness guide published by ANSSI with contributions from the CNIL "Ransomware attacks, all concerned".

In order to increase its participation, the CNIL joined the Cyber Campus in 2022, which brings together the main French players in the cyber domain. It has also strengthened its relationship with the public interest group *Actions contre la cybermalveillance* (ACYMA), which aims to combat acts of cyber crime based on the [cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr) system. CNIL has been a participating member since March 2022.

The CNIL is also a member of associations such as the EBIOS Club and CESIN, and is involved in key cybersecurity events such as the International Cybersecurity Forum (FIC).

### Ransomware attacks



#### FOCUS

Ransomware, or cryptolockers, are malicious programs that prevent victims from accessing their data, by encrypting it and then demanding payment of a ransom in exchange for the decryption key. Ransomware is often transmitted through an email attachment or links that download software or content. Once present in the host computer system, this program will encrypt all accessible files, making them unreadable. In the case of a corporate network, the software will seek to propagate on all accessible resources.

Ransomware is widespread because it is very profitable for attackers. While this type of attack is sometimes opportunistic, with ransoms generally corresponding to a few hundred euros, larger entities are increasingly targeted for amounts up to several million euros.

Some ransomware attacks use known security flaws in order to propagate through corporate networks and multiply the damage. In particular, by making their victims' servers, software and data inaccessible, ransomware attacks make critical services (website, user or internal services) unavailable, very often leading to alteration and/or loss of availability of personal data, which may constitute a personal data breach.

**Commission nationale de  
l'informatique et des libertés**

3 place de Fontenoy  
TSA 80715  
75334 PARIS CEDEX 07  
+33 (0)1 53 73 22 22

[www.cnil.fr/en](http://www.cnil.fr/en)

[www.cnil.fr/fr/cybersecurite](http://www.cnil.fr/fr/cybersecurite)