Cybersecurity

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr
www.cnil.fr/en

GDPR, A CYBERSECURITY INSTRUMENT

INFORMATION SECURITY, AN OBLIGATION SINCE 1978, A REINFORCED FRAMEWORK WITH THE GDPR.

Security is one of the fundamental principles of the Data Protection Act.

GDPR includes reinforced security requirements. It has also confirmed the role of data protection authorities in supporting all companies and administrations in in this area.

SECURITY OBLIGATIONS UNDER GDPR
Implement technical and organisational measures to secure data
Keep a record of personal data breaches
Conduct a data protection impact assessment > For certain sensitive processings
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 European text to impose specific cybersecurity obligations to all organisations, regardless of their size or sector, and subject to enforcement powers of an authority.

In case of non- compliance :

Administrative fine of 20 million euros or 4% of turnover

The CNIL supports administrations and companies in the consideration of computer security.

The security principle, which has been 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 assessments, codes of conduct or certification.

FIGURES

2,825
data breach notifications
in 2020. **+24%** vs. 2019.

More than
500
Data breach notifications
related to a ransomware attack received in 2020.
20% of the total.

2/3
of the sanctions
issued by the CNIL are related to non-compliance with the security requirement. More than **40%** of these sanctions are taken on this sole basis.

3X more
data breaches
related to cryptolocker attacks on healthcare institutions (hospitals, clinics, care facilities, laboratories, etc.).

FOCUS

What is a Privacy Impact Assessment (PIA)?

The PIA is a tool to build a processing operation that complies with the GDPR and respects privacy. It has to be conducted 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. 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 GDPR.

Reade more https://www.cnil.fr/en/privacy-impact-assessment-pia

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. Every year, the CNIL is notified of numerous data breaches that can have serious consequences. The CNIL fully plays acts primarily in 4 areas:

1 **Raising awareness among the general public**

2 **Providing guidance to professionals**

3 **Systematic checks and deterrent sanctions**

4 **Participation in the cyber ecosystem,** Notably through its collaboration with the French National Cybersecurity Agency (ANSSI) and its presence at various thematic events

Raising awareness among the general public

In order to raise public awareness on security, the CNIL has developed various resources. It has published a guide "How to protect my data?" and makes practical information available on its website, including:

- Phishing: detecting a malicious message
- Preventing, spotting and reacting to the hacking of your social accounts
- How to react in case of webcam blackmail
- Good practices to better protect your online identity
- How to react to identity theft
- 10 tips to stay clean on the web
- The CNIL's advice for a good password
- Private browsing to limit the risks of hacking into your online accountse

The CNIL is also setting up partnerships with civil society and businesses, in particular through the Educnum group, launched in May 2013. It brings together various players in the fields of education, research, digital economy, civil society, corporate foundations and other institutions, to promote and support actions aiming at fostering a digital citizen culture.

Providing guidance to professionals

Compliance with data protection rules is often the first step in implementing a cybersecurity policy. This is why the CNIL regularly publishes guides to assist data controllers and their processors, such as:

- a recommendation on passwords;
- a guide to personal data security;
- the guides on data protection impact assessments and the PIA software;
- a security checklist;
- a guide for developers, published on the GitHub platform;
- regular publications of the "Quarterly data breaches" which provide good practices to avoid some breaches or limit their consequences (SQL injections, credential stuffing, president fraud);
- the cyberattack awareness guide published by the ANSSI with the contribution of the CNIL "Ramsomware attacks, all in together";
- best practices on software (e.g. Elasticsearch).

A specific support for small and medium-size enterprises

The CNIL provides SMEs with different tools on its website, such as the GDPR guide published together with Bpifrance, benchmarks, the guide to data retention periods, a simplified record of processing operations or practical information.

To maximize 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.

FOCUS

Ransomware attacks

Ransomware, or cryptolockers, are malicious programs that prevents the victim's access to their data, by encrypting it with a key known only to the attacker, who will then ask for a ransom to be paid in exchange for the decryption key.

It is often transmitted through an email attachment or links that download software or content.

Once present on its "host", the target terminal, this program will encrypt all accessible files and make 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. If this type of attack is sometimes opportunistic, for ransoms generally corresponding to a few hundred euros, large entities are increasingly targeted for amounts that can reach several millions of euros.

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

Systematic checks and deterrent sanctions

2/3 of the sanctions since 2017 involve a breach of the security obligation.

More than 40% of the CNIL's sanctions are taken on this sole basis.

The most frequent infringements

- **data freely accessible by modifying the URL (lack of authentication, predictable URL)**, e.g. when a number modification in the address bar enables access to other people's documents;
- **a password policy which 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;**
- **insufficient testing to verify the absence of vulnerabilities before rolling out a new system.**

Information security is systematically covered in the 300 formal inspections procedures conducted each year. For instance, compliance with basic principles is checked (passwords, database and network security, etc.), as well as the documentation on personal data breaches (which is a new obligation under the GDPR).

Awareness still needs to be raised

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

The CNIL has noted increased awareness on cybersecurity issues within organisations. However, basic good security practices are not systematically implemented. In particular, medium-sized organizations, which are often insufficiently equipped in the field of information security, are particularly affected by the increasing number of ransomware attacks.

The CNIL has also noted shortcomings linked to the failure to deploy adequate encryption solutions, both during its inspections and in the data breaches which have been notified. The implementation of these solutions must become systematic.

DATA BREACH NOTIFICATION

What is a data breach?

According to GDPR, a personal data breach is “a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed”. This consists in any security incident, whether malicious or not and whether intentional or unintentional, that results in a breach of the integrity, confidentiality or availability of personal data.

A few examples:

- **accidental deletion of medical data of 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 a school database and modification of the results obtained by pupils.**

+24% data breaches notified to CNIL in 2020 compared to previous year. On average, over 11 notifications received per business day.

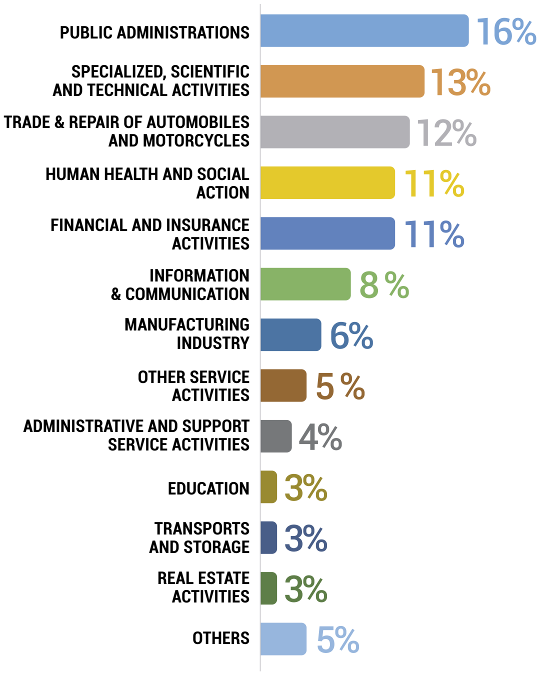
THE GDPR REQUIRES DATA CONTROLLERS TO:

> document personal data breaches internally

> notify the CNIL when the breach results in a risk to the rights and freedoms of individuals within 72 hours;

> inform the persons concerned where this risk is high

Sectors affected by data breaches:



Nature and causes of notified data breaches

69 % of the data breaches notified concern a **loss of confidentiality**.

Although personal data breaches can also result, from a loss of integrity or availability, such breaches are still rarely notified by controllers.

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

The data breach notification obligation concerns breaches whose origin is accidental or unlawful. The majority of notifications received in 2020 concern data breaches originating from a malicious external act (hacking, theft of a physical medium, or fake tech support scams).

HACKING IN 2020

> **47%** dof all notifications to the CNIL, representing **1,315** notifications. (+70% vs. 2019)

> **94%** originate from external malicious acts.

The most common attack is the ransomware attack.

HELPFUL RESOURCES

- **Computer emergency response team - in French:** www.cert.ssi.gouv.fr
- **ANSSI (National cybersecurity agency) - in French:** www.ssi.gouv.fr
- **Assistance and prevention on digital security:** www.cybermalveillance.gouv.fr

Commission nationale
de l'informatique
et des libertés
3 place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
(+33) 01 53 73 22 22

www.cnil.fr

www.cnil.fr/fr/cybersecurite

AGENCE LINÉAL - 03 20 41 40 76

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr
www.cnil.fr/en