Violations of personal data: 5 years of GDPR

27 march 2024

Since May 25, 2018, personal data breaches that may create a risk to the rights and freedoms of individuals must be notified to the CNIL. Five years after the' entry into application of the GDPR, the CNIL draws up a first quantified assessment.

The security of personal data is a major issue for all public and private organizations, as well as for all individuals. The GDPR requires that personal data breaches be notified to the CNIL as soon as a risk is created for the rights and freedoms of data subjects. Organizations are required to put in place means to allow for the detection of security incidents. They then need to be able to qualify them, or not, as data breaches.

> One data breach corresponds to a loss of **availability**, d'**integrity** or of **privacy** personal data, whether its origin is **accidental** or the consequence of' **malicious action**.

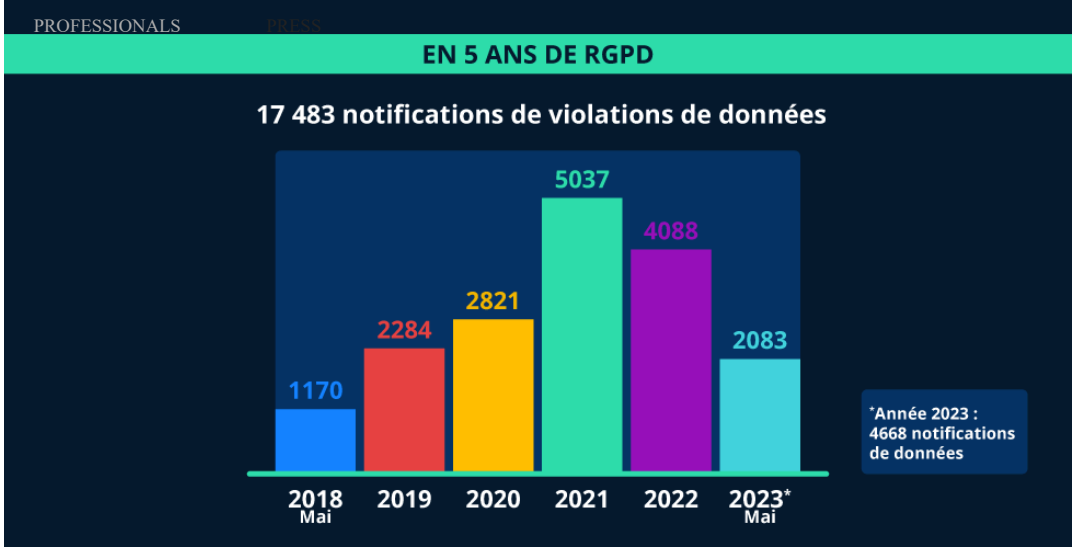
The rapid development of digital usages and data exchanges is expanding the possibilities for data from employees, consumers, citizens, patients or others to be subject to' violation. Some violations are likely to' engender significant risks, such as financial for example, when a hacker intercepts credit card data.

This is why the GDPR requires entities that are subject to a breach to take steps to limit the consequences. In particular, if the risks are high, they are required to INFORM the persons concerned, if possible, individually and to advise them on how to protect themselves against these risks.

The CNIL draws up below a first quantified balance sheet covering **may 2018 to May 2023**.

The balance sheet of 17,483 data breaches reported in 5 years

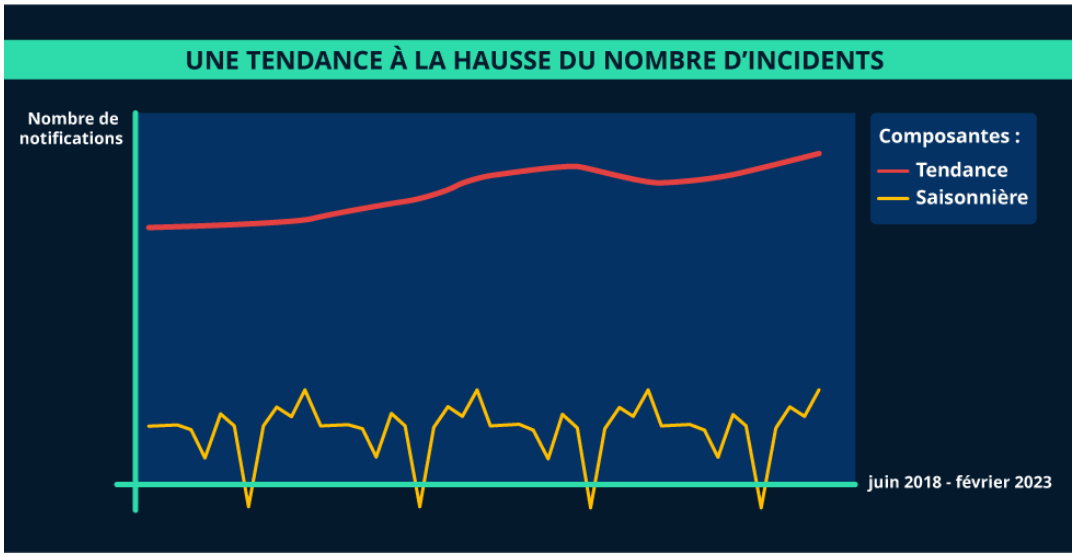
A growing number of violations received



Consult in PDF format

Between May 2018 and May 2023, the CNIL received 17,483 notifications of data breaches. This volume does not reflect the actual number of incidents since a single event, such as a piracy, can give rise to multiple notifications. This often corresponds to situations where a provider is affected by an attack and notifies its customers, in accordance with the GDPR, who themselves make their own notifications.

By grouping the notifications related to the same origin, it appears that **the number of data breaches notified to the CNIL has been increasing over the years**. On this note, it is however difficult to distinguish between the best consideration of the GDPR by stakeholders and a possible amplification of threats to personal data.



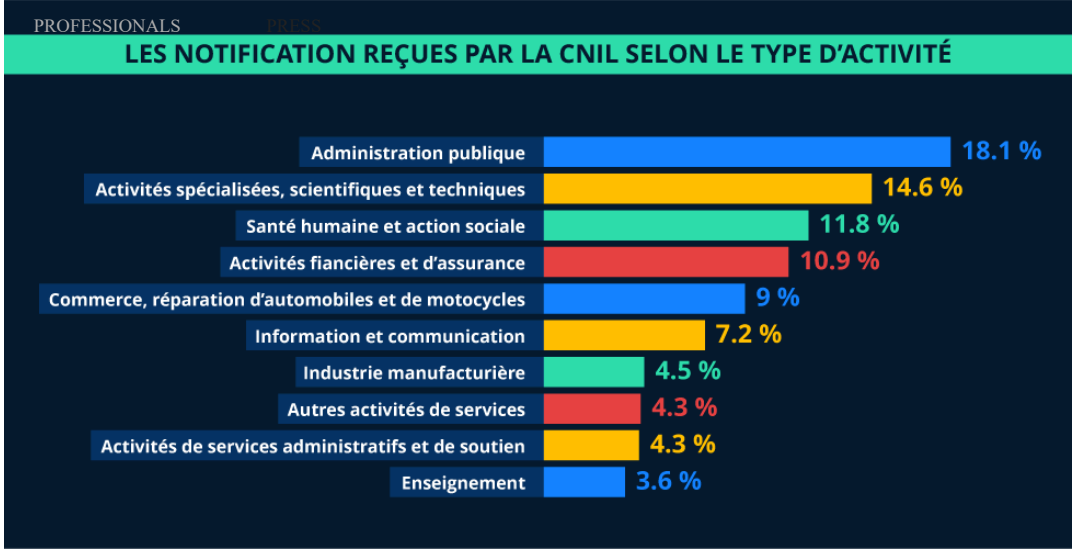
Note : the trend is the sliding average of the number of notifications received by the CNIL corrected for the series resulting from the same incident.

Consult in PDF format

Distribution by sector and type of activity

The private sector is responsible for about two thirds of the reports of violations at the CNIL of which 39% are SMEs. Le **public sector** represents as for him **22 %** of notifications.

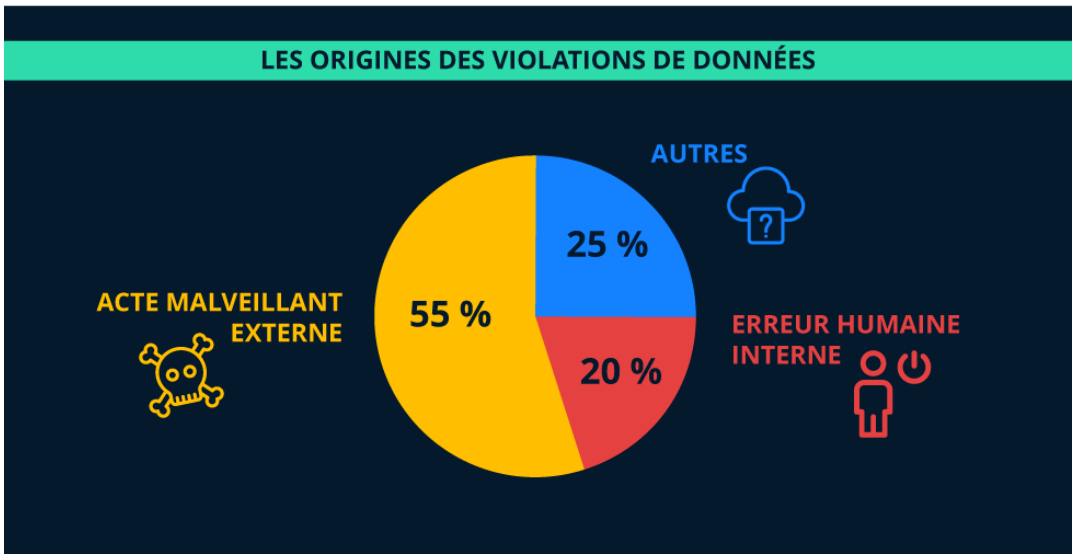
As regards the breakdown by activity, general government accounts for 18% of notifications. Specialized, scientific and technical activities are the most represented in the private sector, followed by financial and assurance activities. **These are sectors strongly linked to personal data**. Similarly, activities related to human health also account for 12 % of the notifications.



Consult in PDF format

These figures reflect only'a part of the security incidents that occur in France. Indeed, the significant presence of data protection delegates in some sectors, the taking into account and the'appropriation of the GDPR in others, etc, have a direct impact on the representation of this or that activity. Thus, the sectors most represented do not necessarily suffer more'incidents than the others and/or do not protect personal data less well. The increase in detection and processing actually leads to an increase in this visible part of the'iceberg.

The origins of data breaches



Consult in PDF format

On the origins of data breaches, the trends observed since 2018 correspond to those of the progress report carried out 4 months after the entry into force of the RGPD and the interim reports published in the annual reports of the CNIL.

More than half of notified violations find their **origin in piracy** : the **ransomware** are in the front row, followed by attacks by **phishing**. The latter are generally prior to other intrusions, on the same system or even on systems of' other controllers. The analysis shows that the **public sector** is more affected by the'**phishing**, while the **private sector** is more concerned with the **ransomware**.

Les **lost or stolen equipment**, the **undue shipments** and the **non-voluntary publications** they are the other most frequent sources of data breaches.

Two major trends are emerging :

- Intentional hacking and thefts attributable to a malicious third party ;
- Involuntary errors of'one or more persons acting on behalf of the data controller.

In other cases, it is most often unknown or not determined by the notifying ORGANISM's or malicious internal'acts.

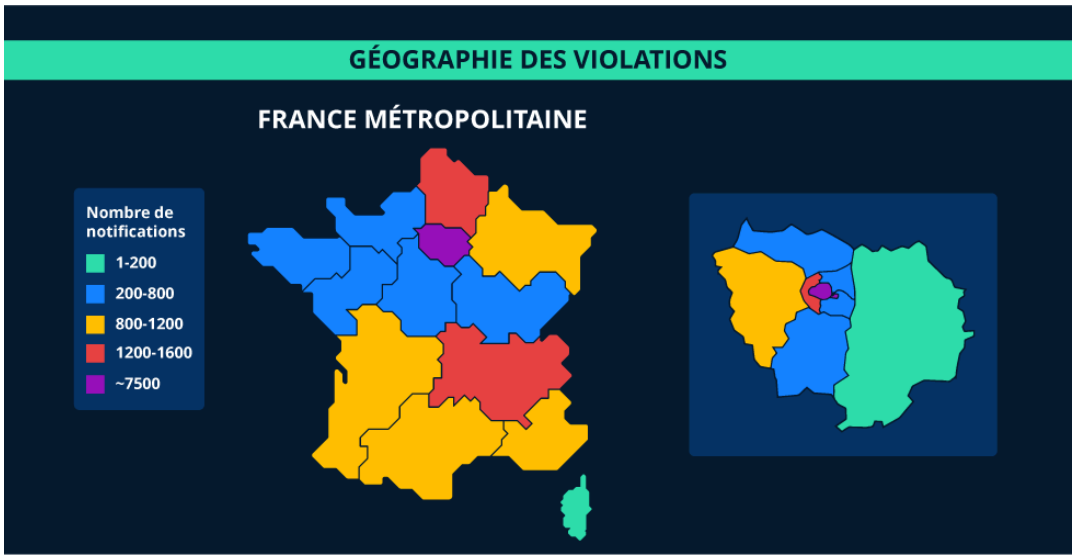
To prevent most of these incidents causing personal data breaches, the CNIL recalls that'il is essential :

- to think about safety from the launch of'a project ;

- to systematically take minimum measures for data security ;
- d' regularly carry out security updates on' operating systems, application servers, or databases ;
- d' regularly inform staff about the risks and challenges of cybersecurity.

The personal data security guide the CNIL recalls the basic precautions that should be implemented in a systematic way by professionals.

The geography of violations



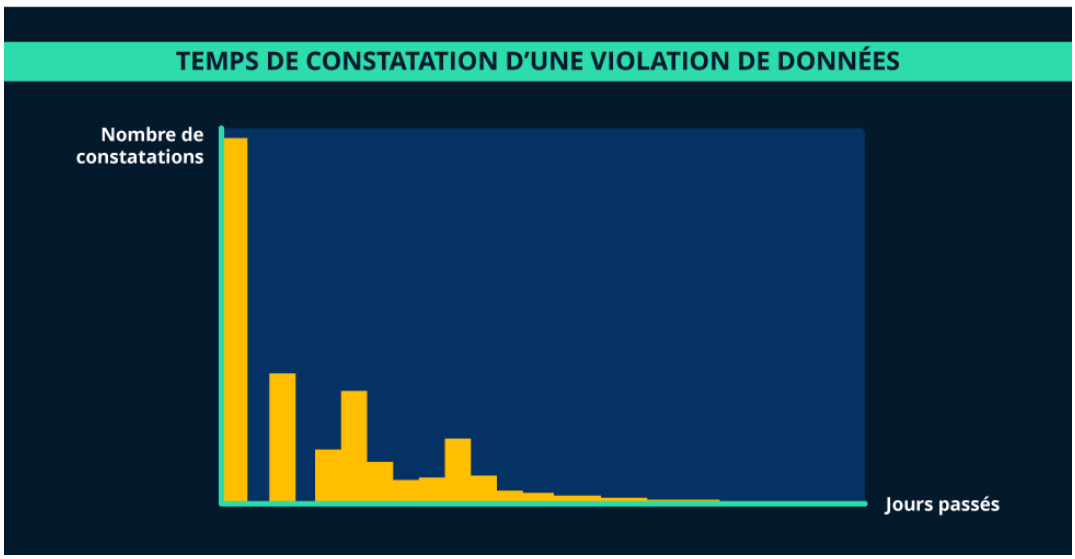
Consult in PDF format

The distribution of notifications of personal data breaches within the'hexagon is not homogeneous. A concentration of the latter is observed in the Ile-de-France region, followed by the Hauts-de-France and the Auvergne-Rhone-Alpes region.

In order to understand this distribution, it should be taken into account that the notification is made by the controller, even if the' incident causing the S' violation occurred in a secondary, geographically distant facility. **Thus, this geographical distribution corresponds to the economic density of the territory, in particular the density of the head offices.** It therefore does not allow conclusions to be drawn on any particular threat or trend.

The temporality of notifications

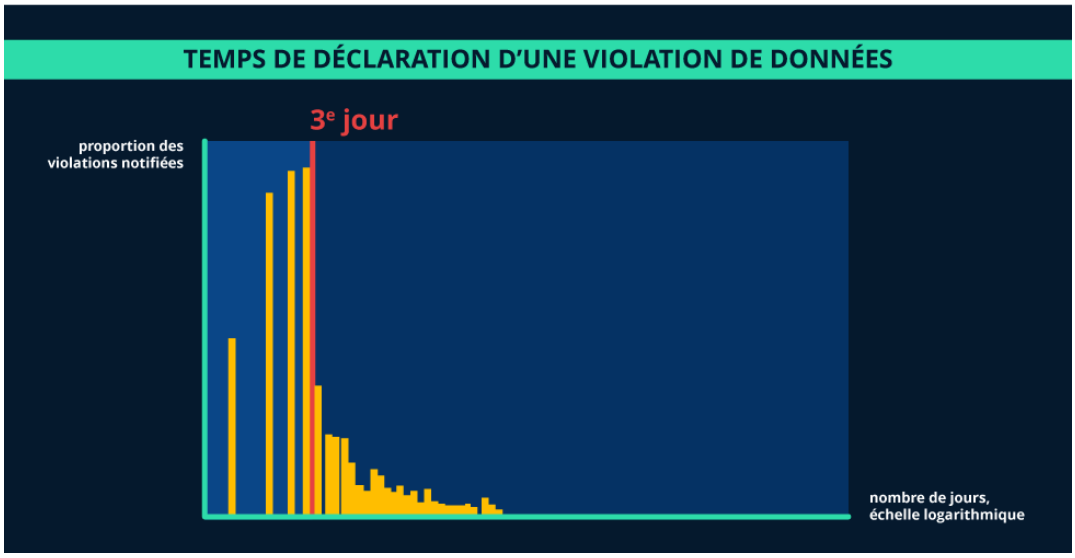
On average, an organization takes 113 days to find a violation. This figure is naturally driven upwards by situations where it sometimes takes several months, if not years, to realize that'a violation has occurred. **In fact, half of the violations are found in less than 10 hours.**



Consult in PDF format

In the event of a personal data breach, the controller shall notify the relevant breach to the competent supervisory authority as soon as possible, and where possible, 72 Hours at the latest after becoming aware of it (article 33.1 of the GDPR). Where notification to the's supervisory authority does not take place within 72 hours, it shall be accompanied by the reasons for the delay.

In fact, **half of the notifications are made within this period**. Violations are reported for 75% of them within 11 days of the incident being classified.



Consult in PDF format

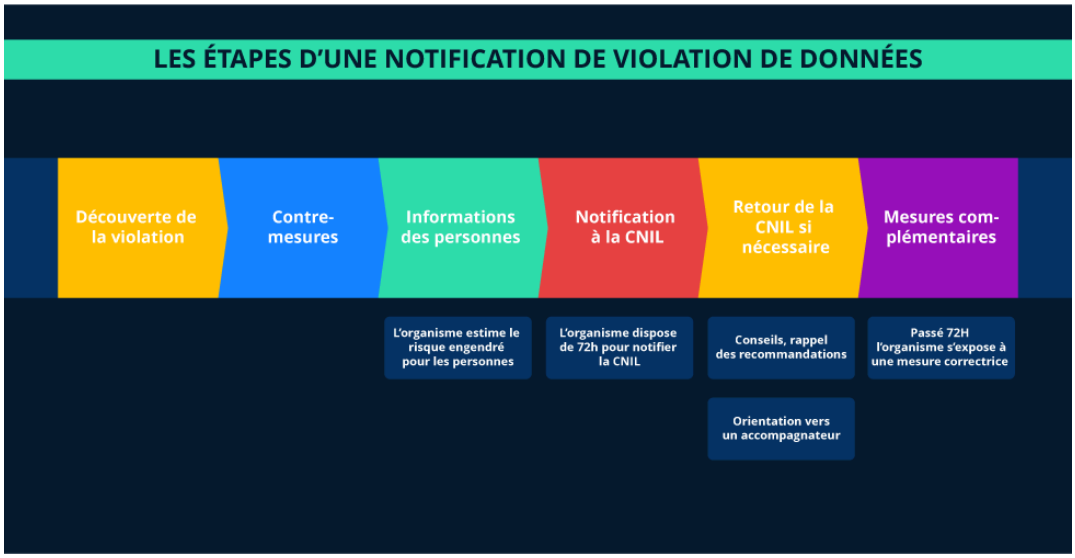
In case of delay, the **main reasons** are :

- the **ignorance of the CNIL notification obligation**, the learner's registrants when filing a complaint or when contacting their cyber insurance for example,
- the **willingness of organizations to wait for tangible elements and expert results.**

Having regard to the CNIL, it is preferable to notify the violation within the 72-hour period, even if it means providing only partial elements, and, which may be subsequently completed or even deleted, in the event that the violation is not proven.

Without legitimate reason, non-compliance with the' notification obligation within 72 hours constitutes a breach of the GDPR, which can be sanctioned by the CNIL. Such a breach is punishable by'a fine of 10 million'euros or 2 % of the turnover'. If the management of'a violation by the controller reveals wilful negligence or a manifest will to hide elements, the CNIL will adopt a repressive approach against it.

The role of the CNIL



Consult in PDF format

In its processing of notifications, the CNIL favors the accompaniment of actors. Its purpose is to assist the professionals concerned to take all measures to limit the consequences of'a violation, for the persons concerned in the first place, as well as for the professionals themselves. In addition, it can provide advice on preventive measures in the field of cybersecurity.

When necessary, the CNIL contacts the organizations to :

- **Verify that measures have been taken** before and /or after the violation :
  - it indicates to the manager, the improvements to be implemented for example on the'use of' algorithm adapted encryption or' optimization of password management ;
  - it also sends those responsible to the police services to file a complaint, or to the platform cybermalveillance.gouv.fr to find information or a service provider.

- **Assess the need, provided for by the GDPR, to provide information to people.** For each notification, the CNIL estimates the risk generated for people and may then be led to recommend to the'organism to inform them of the violation.

It is always possible to contact the services of the CNIL in charge of the management of notifications of personal data breaches by email at' violations@cnil.fr.

To deepen

- Violations of personal data
- All the contents of the CNIL on cybersecurity