Notification of personal data breaches

Law no. 1.565 of December 3, 2024 introduces a new obligation for data controllers: they must notify **any personal data breach of which they have become aware** that is **likely** to result in a **risk to the rights and freedoms of the affected individuals**.

This notification **must** be made to the **APDP** in order to ensure that the rights and freedoms of the people affected by the breach are preserved.

In some cases, the notification may also be accompanied by a **communication** to the people affected by the breach.

A data breach is a security incident, but not every incident constitutes a data breach.

It is therefore important to first understand what the Law means by a data breach before determining whether a notification of the incident is necessary and, in the most serious cases, whether a communication to the affected individuals must be made.

What is a personal data breach?

A data breach is a security incident involving personal data held by a data controller. In accordance with the three classic security principles, these breaches can be classified into three categories:

« ***Confidentiality breaches*** »: occur in the event of disclosure or unauthorized or accidental access to personal data.

Examples :

- the theft of a lawyer's professional laptop containing client files
- mistakenly sending an e-mail containing personal data to persons not authorized to access these data
- the online publication of a company's personal data following a hacking attack
- the recovery by an unauthorized third party of personal data contained in documents that had been thrown away without prior destruction

« ***Integrity breaches*** »: occur in the event of unauthorized or accidental alteration of personal data.

Example :

- an unauthorized third party accesses a file and modifies/deletes its content
- an employee inadvertently enters incorrect information in a database (human error during data entry) (e.g. wrong date of birth or social security number)
- when exporting or migrating data (incorrect format conversion), fields are misinterpreted or truncated, resulting in a loss of accuracy

« ***Availability breaches*** » : are the accidental or malicious loss or destruction of personal data, or their encryption by an unauthorised third party.

Examples :

- a hacker encrypts the customer database of a data controller who has no other copy of it
- the only copy of personal data held by a data controller has been deleted by a hacker
- a non-duplicated database is unavailable for technical reasons

CONFIDENTALITY	INTEGRITY	AVAILABILITY
Only authorized persons should have access to data	Data must not be altered during collection, use, transfer, etc.	Access to personal data must be guaranteed in terms of both time and quality

What are the main types of data breach?

The main types of data breach are as follows:

- **Unauthorised access**: people gain access to data without permission, often through hacking or identity theft.
- **Accidental leakage**: data are shared or exposed by mistake, for example via an e-mail sent to the wrong recipient or a misconfigured system.
- **Data theft**: information is stolen intentionally, often for the purposes of fraud, blackmail or resale.
- **Data loss**: data are deleted or disappear as a result of technical failure, human error or physical damage.
- **Ransomware**: malicious software encrypts system data in return for a ransom payment.
- **Cloud intrusion**: data hosted in online storage environments are compromised.
- **Internal breaches**: unauthorised employees or partners access or disclose data.

Which data breaches are covered by this notification obligation?

Not all data breaches have to be notified to the APDP.

Article 32 of Law no. 1.565 of December 3, 2024 stipulates that the data controller must notify the APDP of **any data breach of which it has become aware and which is likely** to pose **a risk to the rights and freedoms of the affected individuals.**

What is meant by « becoming aware of a breach »?

The independent European Article 29 Working Party has considered in its « *Guidelines 9/2022 on personal data breach notification under GDPR*[1] » that the controller has become aware of a breach when it has a **reasonable degree of certainty** that a security incident has occurred and that the said accident has led to personal data being compromised.

This moment will depend on the **circumstances of the specific breach**.

Indeed, while in some cases it will be relatively clear from the outset that a breach has occurred, in other cases it may take some time before it can be determined whether personal data have been compromised.

Example 1: a data controller is contacted by a hacker asking for a ransom to recover its data.

If, after checking its system, the controller finds that it has indeed been hacked, it will have clear evidence that a data breach has occurred, and will be deemed to have become aware of the breach.

Example 2: an employee informs his employer that he has lost an unencrypted USB key. The employer is deemed to have become aware of the breach at the time, even if it is not yet in a position to know whether unauthorized persons have gained access to the data contained on the drive.

Example 3: a third party informs a data controller that they have received an e-mail from them which was not intended for them. The data controller may then need a little time to check that this e-mail has indeed been sent to a recipient in error.

The data controller will be deemed to have been aware of the violation at the time he carries out these checks.

Where the controller is required to carry out an investigation to determine whether a breach has actually occurred, this initial investigation period should begin **as soon as possible** after the alert.

[1] The Article 29 Working Party was and independent European Union advisory body on data protection and privacy until May 25, 2018 before being replaced by the European Data Protection Board.

What is meant by a « breach likely to result in a risk to rights and freedoms »?

In some cases, the **breach may have no impact** on the rights and freedoms of the individuals concerned.

Examples :

- the personal data affected by the breach are already publicly available
- the deletion of data that had been backed up and immediately restored
- the loss of data protected by a state-of-the-art encryption algorithm, if the encryption key is not compromised and a copy of the data remains available
- company operations are disrupted by a power cut that renders personal data unavailable for just a few minutes

As there is no risk to the persons concerned, such a breach does not have to be notified to the APDP. It must, however, be recorded in the data breach register kept by the data controller.

In other cases, however, the breach presents a **low, medium** or **high** risk to the rights and freedoms of the affected individuals.

Examples :

- patient records held by a hospital are unavailable for more than 24 hours following a hacking attack
- the bank details of a company's customers are stolen and published online
- the personal data of a large company's employees are sent to the wrong list, which includes a large number of recipients

While notification may not initially be required because there is no **likely** risk to the rights and freedoms of individuals, a risk may emerge over time.

Example: when an employee informs his employer that he has lost an encrypted USB key, the data controller may decide not to notify the data breach when the encryption key remains in his possession and the personal data affected do not constitute a single copy.

However, if it subsequently becomes apparent that the encryption key has been compromised, the personal data will become accessible. The data controller will therefore have to notify this breach because of the risk it is likely to pose to the rights and freedoms of the affected individuals.

It is therefore important to **always reassess** the absence of initial risk.

[For more information, refer to the factsheet **Assessing the risk of a data breach in 5 steps**]

When is the notification due?

Once it is aware of the breach, the data controller must notify the APDP **as soon as possible**, and where feasible, no later than **72 hours after having become aware of it.**

What about the data processor?
The processor **must notify** the controller of **any personal data breach as soon as it becomes aware of it**. However, the processor does not have to assess the likelihood of a risk arising from a breach before notifying the controller. The data controller remains responsible for notifying the APDP, even if the breach has occurred at the processor's premises.

The data controller may not have all the information concerning a breach within 72 hours of becoming aware of it, particularly in the case of a complex breach. In such cases, a **notification in phases** is possible, with prior notification of the APDP within 72 hours with a brief summary of the incident, followed by the provision of additional, more detailed information.

If the notification is not made within 72 hours, the reasons for the delay are given.

What must the notification contain?

Mandatory information

The notification sent to the APDP must contain the following information:

- the **nature of the breach** including, where possible, **the categories and approximate number of data subjects concerned** by the breach;
- the **name and contact details of the data protection officer** where the latter has been appointed or **another contact point** where **more information** can be obtained;
- the **likely consequences** of the breach;
- the **measures taken** or proposed to be taken by the controller to **address the breach**, including, where appropriate, measures to mitigate the possible adverse effects.

In addition to this mandatory information, the data controller may also provide specific advice to those affected on how to protect themselves from the possible consequences of the breach.

Example: resetting passwords

The data breach registrer

The data controller **must document** any personal data breach, even when it is not required to notify the APDP.

This documentation must indicate :

- the **facts** relating to the breach
- its **effects** and
- the remedial **measures** taken.

It is also advisable to document the **reasoning for the decisions taken in response to the breach**, in particular where the controller has not notified the data breach, the reasons why it considered that the breach was unlikely to give rise to risks.

This data breach register may be a separate register or be part of a more general register of security incidents.

When should the people affected by the breach be informed?

If the breach is **likely** to result in a **high risk to the rights and freedoms** of a natural person, the controller must also notify the data subject of the breach **as soon as possible**.

The assessment of the high risk is made in the light of a particular incident and is based on the consequences arising from it.

It therefore takes into account, in particular:

- the **type** of breach
- the **sensitivity** and **volume** of personal data
- the **ease of identification** of individuals
- the **severity of consequences** for individuals
- the **likelihood of its recurrence**

If in doubt, the data controller should err on the side of caution and make a communication.

What should the information provided to the affected data subjects contain?

The information to affected individuals must describe the **nature** of the breach in **clear terms** and must contain the following information:

- the **name and contact details of the data protection officer** where the latter has been appointed or **another contact point** where **more information** can be obtained;
- the **likely consequences** of the breach and
- the **measures taken** or proposed to be taken by the controller to **address** the breach, including, where appropriate, measures to mitigate its possible adverse effects.

If the data controller has not communicated the data breach to the affected individuals, **the APDP may order it to do so**.

This information may be **supplemented** by recommendations for individuals to mitigate the potential negative effects of the breach and enable them to take the necessary precautions.

How to communicate with the affected data subjects?

In principle, information should be provided **directly** to the affected individuals, unless this would require disproportionate effort.

This information must be **clear** and **transparent**. It is therefore recommended that it does not contain any other information so as not to dilute the message.

Examples :

- direct messaging (e-mail, SMS, direct message)
- prominent website banners or notification
- postal communications
- prominent advertisement in print media

Depending on the circumstances, the data controller should use **several methods of communication**, rather than a single channel, in order to **maximize the likelihood of the information actually being communicated.**

What are the exceptions to the obligation to inform the affected data subjects ?

Notification of a data breach need not be made if **one of the following 3 conditions** is met:

Condition 1: the data affected by the breach have **previously** been subject to **technical and organizational protection measures** which render the said data **unintelligible** to any person not authorized to access them.

Example : data encryption

Condition 2: the duty to inform the data subject individually would involve **disproportionate efforts**.

Example : the data controller has no information enabling him to contact the individuals

In such cases, it is recommended to make a **public communication** or take a similar measure, whereby the individuals are informed in an equally effective manner

Condition 3: the **subsequent measures** taken by the controller **ensure that the risk is no longer likely to materialize.**

Example : resetting stolen passwords

What is the penalty for failing to comply with the obligation to notify a data breach?

In the event of a **breach of the obligation to notify a data breach** and, where appropriate, to **communicate it to the affected individuals**, the organization may incur an administrative fine of up to **5,000,000 Euros or, in the case of a company, up to 2% of the previous year's total worldwide annual revenue, whichever is the highest.**

[For more information, refer to the factsheet **How to manage a data breach?**]

in a nutshell: