July 2025

The main data breaches: obligations and advice on how to prevent them

What is a data breach?

According to Article 32 of Law no. 1.565 of December 3, 2024, a personal data breach is a **security incident** (accidental or unlawful) resulting in:

- the **destruction, loss** or **alteration** of personal data;
- the **unauthorised disclosure of** or **unauthorized access to** personal data.

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 breach of which it is aware and which is likely to result in a risk to the rights and freedoms of the affected individuals.**

In accordance with the three classic security principles, these breaches can be classified into three categories:

- a « ***breach of confidentiality*** *»:* occurs in the event of unauthorised or accidental disclosure or access to personal data;
- a « ***breach of integrity*** »: occurs in the event of unauthorised or accidental alteration of personal data;
- an « ***breach of availability***»: corresponds to the accidental or malicious loss or destruction of personal data.

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

In addition, where the breach is **likely** to result in a **high risk to the rights and freedoms** of an individual, the controller must also **inform** this individual of the breach **as soon as possible.**

[For more information, refer to the factsheet **Notification of personal data breaches]**

The assessment of high risk is made in the light of a particular incident and is based on the consequences arising from it. It must be based on objective criteria relating to each of the individuals whose data have been affected by the breach, according to their specific situation. Determining the level of risk is not fixed on the day of the breach, but must be reassessed if the information available to the data controller changes.

This factsheet offers a number of scenarios to help you better understand your main obligations in relation to the breaches you encounter, and our advice on how to prevent breaches from occurring or reoccurring.

What factors should be taken into account when assessing the risks of a data breach?

- **the type of breach** (confidentiality, integrity and/or availability of data)
- **the sensitivity of the data** (health data, financial data, criminal offences, etc.)
- **the volume of data** and/or **affected individuals**
- **the category or categories of affected individuals** (children, employees, people with disabilities, the elderly, etc.)
- **how easy it is to identify the people affected by the breach** (encrypted or non-encrypted data)
- **the field of activity of the data controller** (medical, banking, etc.)
- **existing security measures**
- **the possible consequences for individuals** (identity theft, fraud, damage to reputation, etc.)

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

Error in sending a letter or e-mail

An error in sending a letter or e-mail may be the result of inattention or a computer bug. In all cases, such an error can lead to a breach of personal data, especially when the message contains confidential data.

Scenario 1 : Postal mail or e-mail containing no sensitive or confidential data sent by mistake to the wrong recipient

What is the impact of the breach?

A breach of confidentiality as a person not authorized to have access comes into possession of the personal data of one or more other individuals.

Does the APDP need to be notified?

Yes, if the letter/e-mail contains private data that are not accessible to the public (e.g. address, date of birth), the disclosure of which to unauthorised third parties could pose a risk to the rights and freedoms of the affected individuals. It cannot be ruled out that the person who received the letter/e-mail by mistake might use it (for example, for commercial prospecting purposes).

No if the letter/e-mail sent by mistake does not contain any data the use of which could have negative effects for the affected individuals (for example personal data known to the general public such as information relating to politicians or appearing in official directories).

Do affected individuals need to be informed?

This will depend on the **severity of the consequences** for the affected individuals, in particular the **nature** and/or **volume** of the data disclosed in error.

Scenario 2 : Postal mail or e-mail containing sensitive and/or confidential data sent by mistake to the wrong recipient

What is the impact of the breach?

A breach of confidentiality as a person not authorized to have access comes into possession of the personal data of one or more other individuals.

Does the APDP need to be notified?

Yes, the very nature of the data (**sensitive and/or confidential**) is likely to entail a risk for the affected individuals.

Do affected individuals need to be informed?

Yes, in principle. The risk to affected individuals may be considered high because even if the data controller, after realising the error, asks the recipients of the letter/e-mail to disregard it and delete it immediately, it may in some cases not be certain that this has actually been done and that the file has not been intercepted by a third party.

Organisational and technical measures to prevent such a breach from (re)occurring

- Establish precise internal rules for sending letters/e-mails
- Train staff on how to send letters/e-mails
- Check the recipients of letters/e-mails before sending personal data
- Limit the number of recipients of e-mails containing personal data
- When an e-mail is sent to a large number of people, opt for **« *Bcc* »** (invisible carbon copy) in order to hide from each recipient the list of other recipients of this e-mail
- Do not send sensitive data (e.g. medical data) or confidential data (e.g. banking data) but use secure and encrypted means of communication (e.g. secure e-mails or digital safes)
- Apply the 4 eyes principle when sending sensitive or confidential data by assigning each verification step to a different person
- Favour automatic rather than manual addressing, with data extracted from an available and up-to-date database
- Apply the time-out feature, which allows a message to be deleted/edited within a certain period of time after it has been sent
- Deactivate semi-automatic input when entering e-mail addresses
- (…)

Employee exfiltration of company data

Not all attacks come from external threats. Internal threats are frequent, and employee data theft is a particularly complicated risk to prevent.

What is the impact of the breach?

More often than not, this is a **breach of confidentiality**, as the employee simply wants to copy data belonging to the company for the purpose of using them for his or her own benefit at a later date.

Does the APDP need to be notified?

Yes, even if the intentions of the employee in question are unknown and the data concerned are not sensitive or confidential, the data controller cannot consider that the risk to data subjects is negligible.

Do affected individuals need to be informed?

In some cases, yes. Depending on the nature of the data copied, the consequences of the breach may at best be limited to unwanted commercial solicitation, but in other cases the breach may lead to high risks for the affected individuals (fraudulent use of the data, for example).

Organisational and technical measures to prevent such a breach from (re)occurring

- Define different clearance profiles (based on the principle of « *least privilege* ») depending on the roles and responsibilities of people with access to information
- Require users to authenticate themselves when accessing sensitive personal data
- Deactivate and then delete a user's account as soon as they leave the company
- Regularly review the clearance system (management of obsolete accesses)
- Set all computers to lock automatically after a certain period of inactivity
- Draw up an IT charter for all users of the Information System (employees, trainees, service providers, etc.), detailing good practice and obligations in terms of data security
- Organise regular training/presentations to raise employees' awareness of data security and the use of information systems
- Carry out periodic audits of access privileges to ensure their compliance with the organisation's security policy(ies)
- (…)

Loss or theft of a device

Increased mobility means that nomadic business devices - and the data stored on them - are more likely to be stolen or lost. This can have many consequences, some of them particularly serious, if technical and organisational measures have not been put in place beforehand to prevent these risks.

Scenario 1 : Data encrypted and backed up

What is the impact of the breach? (None, unless the key is compromised)

Thanks to the backups made, the data remain available. There is therefore **no breach of availability.**

Furthermore, as long as the decryption key has not been disclosed or stolen, there is **no breach of confidentiality or data integrity**, as the data are encrypted and cannot be accessed by a third party or altered.

On the other hand, if the key is also compromised, there will be a breach of confidentiality of the data, and potentially a breach of their integrity if the person in possession of them alters them in any way.

Does the APDP need to be notified?

No. As long as the data were protected by a state-of-the-art encryption algorithm (although care must be taken to ensure that the encryption key is not compromised) and the data are quickly restored thanks to the backups made, it is unlikely that this breach will result in a risk to the rights and freedoms of the affected individuals.

Do affected individuals need to be informed?

No. In the absence of a high risk to the rights and freedoms of affected individuals, they do not need to be informed of the breach. Here again, the answer will be different if the key has been compromised. Depending on the **nature, category** or **volume** of the data affected by the breach and the **severity of the consequences** for the affected individuals, it may be necessary to inform them.

Scenario 2 : Data encrypted but not saved

What is the impact of the breach?

If there is no backup, the data are no longer available. There is therefore a **breach of availability.**

On the other hand, there is neither a **breach of confidentiality nor a breach of data integrity** because the data are encrypted, so they cannot be accessed by a third party and cannot be altered. However, if the key is also compromised, there will be a breach of confidentiality and potentially a breach of integrity if the person in possession of the data alters them in any way.

Does the APDP need to be notified?

Yes, most likely, because depending on the data and the affected individuals, their lack of availability could lead to a risk for the rights and freedoms of the affected individuals (disappearance of a medical file, for example).

Do affected individuals need to be informed?

This will depend on an **assessment of the nature** or **volume** of the data made unavailable and the **severity of the consequences** for the individuals concerned.

Scenario : Unencrypted data

What is the impact of the breach?

Violation of confidentiality, as the data are unprotected and can be accessed by any unauthorised person in possession of the device.

Furthermore, this person could voluntarily or involuntarily modify the data, which would constitute a **breach of their integrity**.

Finally, if **there is no backup of the data**, the violation may also constitute a **breach of the availability** of these data.

Does the APDP need to be notified?

Yes. The absence of basic protection measures (e.g. the lack of encryption of data stored on the device) entails a risk for the data subjects affected by the breach. This risk may be all the greater if the data subjects can be easily identified, if they are vulnerable, if there is a large number of them and/or if the data concerned are sensitive.

Do affected individuals need to be informed?

Yes, high risk is very likely. Here again, the data controller will have to take into account the **nature, categories** or **volume** of data affected by the breach, as well as the **severity of the consequences** for the affected individuals.

Organisational and technical measures to prevent such a breach from (re)occurring

- Encrypt all mobile devices
- Set up strong passwords for each device (including a minimum of 12 characters, upper and lower case letters, numbers and special characters)
- Use mobile device management (MDM) solutions
- Use anti-reflection filters
- If possible, back up personal data not on the mobile device but on a central server
- Use a secure VPN
- Make employees aware of the risks of losing or stealing mobile devices
- (…)

Ransomware

Considered to be one of the most popular cyberthreats among hackers, ransomware is malicious software that takes hostage the data contained in a computer system, encrypting and blocking files on servers (information systems) and only sending the key to decrypt them when (theoretically) the user has paid a ransom.

Scenario 1: Protected Information System (IS) (encryption + backup)

In this scenario, the data controller uses encryption at rest to ensure that when data stored in the IS fall into the hands of a hacker, the hacker cannot read them without having access to the encryption keys.

In addition, all the data were backed up.

What is the impact of the breach?

No real risk. There is **no breach of confidentiality or data integrity,** because the data are encrypted so that they cannot be accessed by the hacker without the decryption keys and cannot therefore be altered.

Furthermore, there is **no breach of data availability**, since even if the hacker has encrypted the data, they can be quickly restored thanks to the backups made.

Does the APDP need to be notified?

No. Since the data were protected against unauthorised access by encryption at rest, and since the data were quickly restored thanks to the backups made, it is unlikely that this breach will result in a risk to the rights and freedoms of the data subjects.

Do affected individuals need to be informed?

No. If there is **no high risk** to the rights and freedoms of the data subjects, they do not need to be informed of the breach.

Scenario 2: Unprotected Information System (IS)

In this scenario, data were neither encrypted at rest nor backed up.

What is the impact of the breach?

Breach of availability and potentially of confidentiality and integrity.

In the absence of backups by the data controller, there is a **breach of data availability**. As the data have been encrypted by the hacker, they cannot be restored if the data controller does not have a paper copy or a copy on another medium(s).

Furthermore, if the stored data have not been encrypted at rest, the data controller will have to carry out an in-depth examination to determine whether the hacker was able to access the data, which would also lead to a **breach of confidentiality**.

Finally, if the data have been extracted, it is also possible that **their integrity has been breached** if they has been altered during collection, use, transfer, etc.

Does the APDP need to be notified?

Yes, most likely. The absence of basic protection measures (not encrypting stored data at rest and the absence of regular backups) entails a risk for the data subjects affected by the breach. This risk may be all the greater **if these people can be easily identified, if they are vulnerable, if there are a large number of them and/or if the data concerned are sensitive**.

Do affected individuals need to be informed?

Yes, most probably. Here again, the data controller will have to take into account the **nature, sensitivity** and/or **volume** of the data affected by the breach, as well as the **severity of the consequences** for the affected individuals.

If there is no backup, the data may be lost and will have to be collected again, unless another source is available (e.g. a paper file). This can have particularly dramatic consequences for affected individuals when the data are health data, for example.

In addition, some data, depending on their nature (identity documents or financial data, for example), can be used for identity theft or fraud.

Organisational and technical measures to prevent such a breach from (re)occurring

- Limit the number of attempts to access an account
- Install an appropriate, up-to-date firewall and intrusion detection and prevention system
- Use regularly updated antivirus software
- Install critical updates (security patches) without delay
- Encrypt data stored on all media and systems at rest
- Carry out regular audits of information systems to check compliance with security policies and identify any vulnerabilities
- Institute regular data backup procedures to prevent data loss in the event of attacks
- Train staff in methods of recognising and preventing computer attacks
- Carry out periodic vulnerability and intrusion tests
- (…)

To conclude: Some recommended preventive measures to avoid the risk of data breaches

- staff training
- verification of recipients before sending
- use of secure means of communication
- encryption of equipment and data
- regular backups
- strong authentication
- monitoring access and flows
- software and antivirus updates
- application of the principle of least privilege

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