How to manage a data breach?

A data breach is a security incident involving personal data held by a data controller. 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.**

As there is no such thing as zero risk, it is important to put in place upstream measures to prevent any breach from occurring, as well as an action plan to deal with any incident as effectively as possible and to respond in accordance with the law.

To achieve this, 6 steps are recommended, which can be summarized as follows:

- Prevention
- Detection
- Risk assessment
- Risk mitigation
- Communication
- Post-incident management

Step 1 : Prévention

Better safe than sorry…

A data breach can happen at any time, to anyone. So it is wise to be proactive and prepare for the worst, by putting in place a proper IT security policy.

The 15 basic rules of It security

1. Protection of premises
2. Securing workstations, servers and mobile computing
3. Training and raising awareness of Information System users
4. User authentification
5. Authorization management
6. Supervision for subcontracting
7. Traceability of operations
8. Securing external echanges
9. Regular back-ups
10. Supervision of hardware and software maintenance and end-of-life
11. Alert procedures
12. Security incident management policy
13. Risk analysis
14. Security audits
15. Business continutity and disaster recovery policy

Step 2: Detection

While most incidents occur in just a few seconds, detection generally takes much longer. It is therefore important to have monitoring and alert mechanisms in place so that any abnormal activity that may occur internally can be reported as quickly as possible. Early detection of a breach is essential to minimize its impact.

Examples of suspicious activities:

- Unusual and numerous accesses to files
- Mass data mouvements
- Unauthorized connection attempts
- Unauthorized access to sensitive data
- Unusual network traffic
- Suspicious e-mails
- A request for ransomware

This step must be carried out in consultation with all the players involved (IT team, Human Resources department, external service providers, etc.).

Step 3: Risk assessment

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

As soon as an incident is identified, its scope and impact must be assessed to determine whether it is indeed a data breach and whether the Data Protection Authority and, if necessary, the affected individuals should be informed.

A « *data breach* » questionnaire and a risk analysis matrix drawn up beforehand will be useful in assessing the seriousness of the breach.

Example of a « *data breach* » questionnaire:

- When did the breach occur?
- What is the cause of the breach?
  - internal
  - external
- What is the nature of the breach?
  - accidental breach
  - intentional breach (theft, hacking, etc.)
- What data are affected by the breach?
  - ordinary (identity, addresses, financial characteristics, etc.)
  - sensitive (racial origins, political affiliations, etc.)
- How many people are affected by the breach?
- What is the impact of the breach?
  - breach of confidentiality (disclosure of data or unauthorized or accidental access to data)
  - breach of integrity (unauthorized or accidental alteration of data)
  - breach of availability (accidental or unauthorized destruction or loss of access to data)
- What is the degree of risk to the rights and freedoms of the affected individuals?
  - low risk
  - medium risk
  - high RISK
- Should the APDP be notified?
- Do the affected individuals need to be informed?

Step 4: Risk mitigation

Responding to a data breach is first and foremost about containing and isolating the incident to prevent data from being further compromised and to limit the spread of the incident. An incident response plan drawn up in advance can help you achieve this. It should describe the preventive measures and detailed procedures to be followed.

Examples of actions :

- Disconnect affected devices or software
- Block malicious IP addresses or domains
- Block compromised accounts
- Change passwords
- Set up virtual barriers to contain the incident
- Restore data from backups

It is important to document all actions taken.

Step 5: Communication

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

Article 32 of Law no. 1.565 of 3 December 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**.

This notification must be made **as soon as possible**, and if possible within a maximum of **72 hours of becoming aware of the breach**.

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

In principle, communication should be made **directly** to the affected individuals, unless this would require a disproportionate effort. It must also be **clear** and **transparent**.

Examples of means of communication:

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

The information provided to affected individuals may be accompanied by **recommendations for mitigating the potential negative effects** of the breach and enabling them to take the necessary precautions.

Step 6 : Post-incident management

« Mistakes are wonderful opportunities to learn. » - Jane Nelsen

The data breach has been contained and, if necessary, the APDP has been notified and the affected individuals contacted. All that remains now is to analyze the incident in order to prevent a similar breach from happening again.

This means understanding what happened, why it happened, how it was managed and what can be improved.

It is also important to monitor the corrective actions that have been taken in order to improve them if necessary.

Finally, it will be necessary to learn from the breach and put in place a continuous improvement process, which may include recommendations such as improving staff awareness of safety issues, training, testing or auditing.

The importance of registering data breaches

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 reason why it considered that the breach was unlikely to give rise to risks.

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