PERSONAL DATA SECURITY INCIDENTS AND ASSESSMENT FOR NOTIFYING THE BRAZILIAN DATA PROTECTION AUTHORITY (ANPD)

(Available in Portuguese here)

What is a security incident?

A security incident is any confirmed or suspected adverse event involving a data breach such as unauthorized, accidental, or unlawful access that results in destruction, loss, alteration, leakage of data, as well as any form of inappropriate or unlawful data processing that could put the rights and freedoms of data subjects at risk.

Article 47 of Law No. 13,709/2018 – The Brazilian Data Protection Law (LGPD) – determines that data processing agents must adopt security, technical and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations involving destruction, loss, alteration or communication of data, as well as any form of inappropriate or unlawful processing.

Access the form in this link (available in Portuguese here)

What should be done in the event of a security incident?

- Internally assess the nature and category of the incident, along with the number of data subjects affected, category and quantity of data affected, and any concrete and potential consequences. See the evaluation form on the ANPD website.
- Notify the Data Protection Officer (Article 5, VIII of the LGPD);
- Notify the data controller if you are the data processor, in accordance with the LGPD;
- Notify the ANPD and the data subject, in case of relevant risks or damage to the data subject (Article 48 of LGPD);
- Notify the data subject in case of relevant risk; and
- Prepare documentation for and internal assessment of the incident, as well as measures taken and risk analysis, so as to comply with the LGPD's principle of accountability and responsibility (Article 6, X of LGPD).

What should be communicated to the ANPD?

Article 48 of the LGPD determines that it is the data controller's obligation to inform both the ANPD and the data subject of the occurrence of any security incident that may lead to relevant risks or damage to data subjects.

It is recommended that data controllers adopt a cautious position, so that communication is made even when there is doubt about the relevance of the risks and damages involved. It should be noted that any eventual and proven underestimation of risks and damages by the data controllers may be considered non-compliant with personal data protection legislation.

Information communicated to the ANPD should be clear and concise. In addition to what is prescribed in the LGPD's Article 48, paragraph 1, it is recommended that any notification contain the following information, available in the ANPD's security incident notification form:

- Identification and contact details of the entity or person responsible for data processing;
- Identification and contact details of the Data Protection Officer (DPO) or other associated point of contact;
- An indication as to whether the notification is complete or partial. In case of a partial notification, it should be indicated whether it is a preliminary or supplementary notification.

- Information about the security incident:
  - Date and time of detection of the incident;
  - Date and time of duration of the incident;
  - Circumstances that led to the data breach, e.g. loss, theft, copying, leaking;
  - Description of the personal data and information affected, including the nature and content of the personal data, category and quantity of data as well as the affected data subjects;
  - A summary of the incident itself, indicating the physical location and data storage medium;
  - Possible consequences and negative effects for affected data subjects;
  - Preventive security, technical and administrative measures taken by the data controller in accordance with the LGPD;
  - A summary of measures implemented thus far to control possible damage;

- Any potentially related cross-border issues;
- Other useful information for affected data subjects to protect their data or prevent possible damage.

Additional information can be provided later on if it is not possible to provide all the information at the time of the preliminary notice.

When giving preliminary notice, the ANPD should be informed whether further information will be provided at a later time, and how it will be obtained. The ANPD may also request additional information at any time.

What should be communicated to the data subject, and when?

Data subjects should be notified whenever the security incident could put them at risk or lead to damages.

More objective criteria will be the subject of future regulation and cannot be demanded here as it would be an innovation of the LGPD. Regardless, one can infer from the law that the probability of risk or relevant damage to the data subjects will be greater whenever the incident either involves sensitive data or data from individuals in vulnerable situations (including minors) or has the potential to cause material or moral damage, including discrimination, violation of image and reputation rights, financial fraud and identity theft. Likewise, the volume of data involved, the number of individuals affected, the good faith and intentions of third parties that had access to the data after the incident, and how easily data subjects can be identified by unauthorized third parties should also be considered.

The data controller should internally assess the relevance of risks or damage stemming from the security incident to determine whether the ANPD and data subject should be notified. It is suggested to internally answer the following questions:

1. Has a personal data security incident occurred?

Yes - Next question.

No - There is no need to notify the ANPD if there has been no security incident related to personal data.

2. Are there relevant risks or damages to the individual rights and freedoms of the affected data subjects due to the security incident?

Yes - Notify the ANPD and the data subject.

No - Communication to the ANPD will not be necessary if the data controller can irrefutably demonstrate that the data breach does not pose a relevant risk to the rights and freedoms of the data subject.

What is the timeframe for notifying the ANPD of a security incident?

The LGPD determines that the communication of the security incident must be made within a reasonable period of time (Article 48, paragraph 1), as defined by the ANPD. Although there has been no formal regulation in this regard, the completion of the notification will be considered in any regulatory inspection as a demonstration of transparency and good faith.

While regulations remain pending, the ANPD should be notified of any adverse event and relevant risks as soon as possible, indicated as within two working days of the security incident being detected.

This timeframe was established based on the communication timeframe provided for by Decree No. 9936/2019, and also in view of the need for the ANPD to manage security incidents and harmful consequences that may occur due to delays in containment or mitigation actions.

How should a security incident be communicated to the National Data Protection Authority?

An electronic form is available on the site that can be filled out and submitted via Electronic Petitioning - External User. For more information about submitting the form, access: https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico.