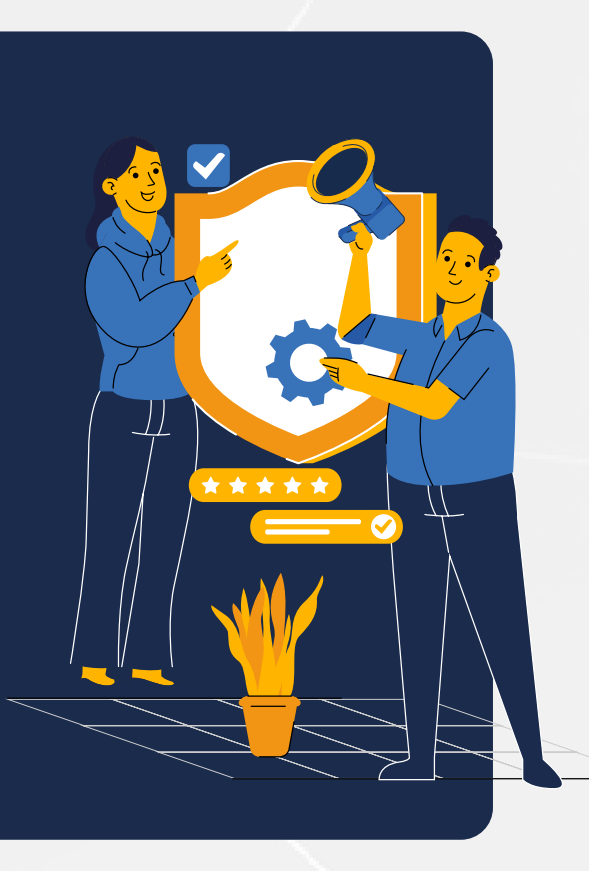
b/luz

EXECUTIVE SUMMARY

Security Incident Reporting Regulation

On April 26, 2024, the Resolution CD/ANPD No. 15 was published, **setting forth the rules for reporting security incidents involving personal data** to the ANPD and to the data subjects. The resolution specifies aspects related to the notification timeframe, establishes procedural aspects, and outlines measures to safeguard the rights of data subjects.



WHAT IS CONSIDERED A BREACH?

The ANPD defines a personal data breach as an adverse event that compromises the **confidentiality, integrity, availability, and authenticity of personal data security**. This may arise from intentional or accidental actions that result in the disclosure, dissemination, alteration, improper loss, or unauthorized access to personal data, regardless of the means in which they are stored. Examples include:

- Sending information to the wrong recipient
- Theft of a data storage device
- Invasion of an information storage system

WHEN MUST BREACHES BE REPORTED?

Chapter III Section I

Security incidents involving personal data and that contain the following characteristics must be reported to both the ANPD and data subjects:

Pose a risk or cause significant harm to data subjects

Defined as those incidents that have the potential to **significantly affect the interests and fundamental rights of data subjects** by:

- Preventing the exercise of rights or the use of a service;

or

- Causing material or moral harm to data subjects

Examples include discrimination, breaches of physical integrity, rights to image and reputation, financial fraud, or identity theft

\+

Meeting at least one of the following criteria

- Sensitive Personal Data
- Financial Data
- Large Scale Data

  Note: Must involve a significant number of data subjects, taking into account the volume of data involved, as well as the duration, frequency, and geographical scope of the data subjects' locations.
- Data concerning children, adolescents, or elderly individuals
- Authentication data in systems
- Data protected by legal, judicial, or professional secrecy

WHO IS RESPONSIBLE FOR REPORTING?

THE DATA CONTROLLER

The data controller is responsible for reporting the security incident involving personal data to both the data subject and the ANPD.

WHAT IS THE REPORTING DEADLINE?

3 business days

Note: Additional deadlines may apply as specified in relevant legislation.

The notification to the ANPD and to the data subjects must be made within three business days from when the data controller becomes aware that the incident has affected personal data

⚠ **Small-sized enterprises** have an extended deadline equivalent to two times the standard timeframe

The information may be supplemented, with justification, within a period of 20 business days from the date of the initial communication.

WHAT INFORMATION MUST BE INCLUDED IN THE INCIDENT REPORT TO THE ANPD?

- Description of the **nature** and **category** of **personal data affected**
- **Contact details** of the Data Protection Officer, or the representative of the data controller
- **Total number of data subjects affected**, specifying the number of children, adolescents, or elderly individuals where applicable
- **Identification of the data controller** and, if applicable, a statement indicating that it is a Small-Sized Enterprise
- **Risks** and **potential impacts** to the data subjects
- Information about the **data processor**, if any
- Reasons for any delay, if the **notification was not made within the prescribed timeframe**
- **Description of the incident**, including the primary cause, if it can be identified
- The **total number** of data subjects whose data is processed and the processing activities affected by the incident
- The **date of the incident** occurrence, if determinable, and the date when the data controller became **aware** of it
- **Technical and security measures taken** or to be taken to reverse or **mitigate the effects of the incident**, taking into account commercial and industrial secrets

WHAT INFORMATION MUST BE INCLUDED IN THE INCIDENT NOTIFICATION TO DATA SUBJECTS?

- **description of the nature and category of personal data affected**
- **risks associated with the incident, including potential impacts on the data subjects**
- **measures that have been or will be taken to reverse or mitigate the effects of the incident, if any**
- **date on which the security incident was identified**
- **contact information for further inquiries and details of the Data Protection Officer, if applicable**
- **reasons for any delay, if the notification was not made within the stipulated timeframe**
- **technical and security measures implemented to protect the data, respecting commercial and industrial secrets**

The notification to data subjects must adhere to the following criteria:

Use of simple and easily understandable language

Notification must be direct and individualized

It may be carried out using the usual means by which the controller contacts the data subject, such as by telephone, email, electronic message, or letter.

? If direct and individualized communication to data subjects is not possible, what are the requirements?

The controller must notify the incident using available means of dissemination such as on their website, apps, social media platforms, and customer service channels. The communication should be easily visible and remain available for a minimum period of three months.

Additionally, the controller must attach to the incident communication process before the ANPD a declaration that notification to the data subjects has been carried out, detailing the means of communication or dissemination used. This declaration must be submitted within three (3) business days from the end of the notification period to the data subjects.

WHAT TO DO IF IT IS NOT NECESSARY TO REPORT THE INCIDENT?

The controller must maintain a record of security incidents, including those not reported to the ANPD and the data subjects, for a minimum period of five (5) years from the date of the event. This period should be extended if additional obligations are identified that require a longer retention period.

WHAT HAPPENS WITH INCIDENTS NOT REPORTED BY THE CONTROLLER THAT THE ANPD BECOMES AWARE OF?

If the incident may cause significant risk or harm to the data subjects, and the controller has not reported the incident, the Authority may initiate an investigation into the situation through a security incident investigation procedure.

SANCTIONS

The ANPD may impose a daily fine to ensure the immediate adoption by the controller of necessary preventive measures to safeguard the rights of the data subjects, in order to prevent, mitigate, or reverse the effects of the incident and avoid the occurrence of serious and irreparable harm or damage that is difficult to repair.

The maximum fine that can be imposed by the ANPD is **BRL 50,000,000.00 (fifty million reais)** as stipulated in the Administrative Sanctions Regulation.

The ANPD may also initiate an administrative sanctioning process to investigate non-compliance with the obligation to report the security incident, which may result in the application of other sanctions provided for in the legislation.

WHAT PROCEDURES WILL THE ANPD FOLLOW AFTER RECEIVING A NOTIFICATION?

1 Receipt of the Incident Notification by the ANPD

2 Conducting Audits or Inspections

The ANPD may, **at any time**, decide to conduct or carry out audits or inspections on data processors to gather additional information or validate the information received

3 Assessment of the Incident's Severity

Based on the information provided by the controller or collected during the audits and inspections, the ANPD will assess the severity of the incident.

4 Determination of Safeguard Measures

After the assessment of the incident's severity, the ANPD may instruct the controller to:

Broadly Disclose the Incident

Through physical or digital means, always considering the need to reach the largest possible number of affected data subjects. This may include printed media, broadcast, or transmission of information via the internet.

when the communication conducted by the controller proves insufficient to reach the affected data subjects

Adopt Mitigation Measures

To ensure the confidentiality, integrity, availability, and authenticity of the affected personal data, as well as measures capable of minimizing the effects of the incident on the data subjects.

DISCLOSE THE BREACH ON THE ANPD'S WEBSITE

The ANPD may publish aggregated statistical information related to security incidents on its website.

5 Initiation of an Administrative Sanctioning Process

Should the controller fail to implement the measures requested, the ANPD may initiate an administrative sanctioning process, which may result in the imposition of fines and other sanctions as described in the law.

6 Termination of the Security Incident Communication Process

The security incident communication process will be terminated if:

1) Insufficient evidence of the incident's occurrence is found;
2) The ANPD determines that the incident does not have the potential to cause significant risk or harm to the data subjects;
3) The incident does not involve personal data;
4) All additional measures to mitigate or reverse the effects generated have been taken; or
5) Notification to the data subjects has been carried out and the controller has taken the relevant measures.

KEY POINTS ON THE COMMUNICATION OF SECURITY INCIDENTS

NOT EVERY INCIDENT REQUIRES NOTIFICATION TO THE ANPD

There is a legal obligation to notify the ANPD only of incidents that may cause significant risks or harm to data subjects. It is the responsibility of the personal data controller to conduct an assessment of the risks and impacts on data subjects resulting from the incident, to determine if notification to the Authority is necessary.

INDICATION OF GOOD FAITH

Voluntary communication of the incident by the controller enhances transparency, cooperation, and good faith of the agent and may be considered as a mitigating factor in any regulatory action by the ANPD.

RESPONSIBILITIES OF A DATA PROCESSOR

Under Article 48 of the LGPD, the duty to report security incidents to the ANPD falls primarily on the data controller. If a data processor identifies a security incident involving data managed under a controller's direction, it is recommended that the processor convey all relevant details to the data controller. Then, the controller may decide whether to proceed with the formal notification to the ANPD.

b/luz