GUIDE ON THE REPORTING OF DATA SECURITY INCIDENTS

This Guide was prepared by the TMT and Privacy and Data Protection team at Azevedo Sette Advogados to serve as initial guidance for a Controller's decision regarding the report of a security incident to the National Data Protection Authority (ANPD).

It is simply a Guide structured in a Q&A format, followed by an initial Checklist. It does not replace professional advice considering the specificities of each case. Therefore, it must not be regarded as a substitute for specialized legal advice.

The Guide is updated until October 8, 2024, so any legislative or regulatory changes occurring after this date should be consulted in addition to this document.

QUESTIONS AND ANSWERS

1. What is a security incident?

It is any confirmed adverse event related to the violation of the properties of confidentiality, integrity, availability, and authenticity of personal data security (Res. CD/ANPD 15/2024, art. 3, XII). In this context, it is relevant to present the following definitions:

- **Authenticity:** property that ensures that the information was produced, issued, modified, or destroyed by a specific individual, equipment, system, body, or entity (Res. CD/ANPD 15/2024, art. 3, II);

- **Confidentiality**: property that ensures that personal data is not available or disclosed to unauthorized individuals, companies, systems, bodies or entities (Res. CD/ANPD 15/2024, art. 3, V);

- **Integrity**: property that ensures that personal data has not been modified or destroyed in an unauthorized or accidental manner (Res. CD/ANPD 15/2024, art. 3, XIII);

- **Availability**: property that ensures that personal data are accessible and usable, on demand, by a natural person or a specific system, body, or entity that is duly authorized (Res. CD/ANPD 15/2024, art. 3, XI);

2. What type of security incident must be reported?

The security incident that may pose relevant risk or harm to data subjects must be reported.

www.azevedosette.com.br

Av. Pres. Juscelino Kubitschek, 1327 | 11º andar | Ed. International Plaza II
04543-011 | São Paulo | SP
Tel +55 11 4083.7600 | Fax +55 11 4083.7601

2.1. When is "risk or significant harm" present?

There is risk or significant harm when the security incident **(a)** can significantly affect the interests and fundamental rights of data subjects **and, cumulatively**, **(b)** involves at least one of the criteria under art. 5, I a VI of Res. CD/ANPD 15/2024.

(a) The security incident significantly affecting fundamental interests and rights will be characterized, among other situations, where **the processing activity may impede the exercise of rights or the use of a service, as well as cause material or moral damage to individuals**, such as any of the circumstances below:

- Discrimination
- Violation of physical integrity
- The right to image and reputation
- Financial fraud; or
- Identity theft

(b) The criteria under art. 5, I a VI of Res. CD/ANPD 15/2024 are:

- **Sensitive personal data:** personal data concerning racial or ethnic origin, religious beliefs, political opinions, membership in a union or a religious, philosophical, or political organization, data related to health or sexual life, genetic or biometric data, when linked to a natural person;

- **Data of children, adolescents, or the elderly:** according to the Statute of the Child and Adolescent (ECA - Law 8,069/1990), a child is defined as a person up to but not including twelve years old, while an adolescent is a person aged between twelve and eighteen years. According to the Statute of the Elderly (Law 10,741/2003), a person aged sixty years or older is considered elderly;

- **Financial data**: personal data related to the financial life of the data subject, including for the contracting of services and acquisition of products;

- **Data for authentication in systems:** any personal data used as credentials to determine access to a system or to confirm the identification of a user, such as login accounts, tokens, and passwords;

- **Data protected by legal or judicial confidentiality:** personal data the confidentiality of which arises from legal norms or judicial decisions;

- **Data protected by professional secrecy:** personal data the confidentiality of which arises from the exercise of a function, ministry, profession or occupation, and the disclosure of which could cause harm to someone; or

- **Large-scale data:** characterized when it involves a significant number of data subjects, considering also the volume of data involved, the duration, frequency, and geographical extent of the location of the data subjects.

Where (a) and (b) are present, under the current regulation, the security incident is considered capable of causing **relevant risk or harm to data subjects** and, therefore, must be reported to ANPD and to the data subject.

2.2. Who are the personal data subjects?

The data subject is the "natural person to whom the personal data being processed refer" (LGPD, art. 5, V). Personal data are information related to an identified or identifiable natural person. In the case of a security incident, the data subjects are the natural persons whose personal data were affected in connection with the incident.

3. Who must report the security incident?

The Controller (LGPD, art. 48). The Report of a security incident is an act of the Controller that informs ANPD and the data subject of the occurrence of a security incident that may pose a risk or significant harm to the data subjects (Res. CD/ANPD 15/2024, art. 3, IV).

Currently, there is no specification in law or regulation indicating whether the Data Protection Officer of the Controller should communicate the incident. Therefore, it is possible for a representative appointed by the Controller for the purposes of the communication to be designated, such as a lawyer with specific power of attorney for this purpose.

This practice can be observed on ANPD's SEI page, where external legal representatives have filed communication reports for Controller companies involved in security incidents. The advantage of using an external legal representative to act on behalf of the Controller for the report is that it protects the Controller from exposure in the market regarding the incident. If it is in the interest of ANPD, however, it may require the Controller to publicly disclose the occurrence (LGPD, art. 48, § 2, I).

4. To whom must the security incident be reported?

The incident must reported to ANPD and to the affected data subjects.

5. What is the deadline for reporting the security incident?

The deadline established in the regulation is **three business days**, counted from the Controller's knowledge that the incident affected personal data. If there is another deadline for incident

reporting provided in specific legislation, the latter must be followed (Res. CD/ANPD 15/2024, art. 6).

For small-scale agents, the deadline for reporting is granted **in double** (Res. CD/ANPD 2/2022, art. 14, II), except when there is potential compromise to the physical or moral integrity of the data subjects or to national security.

Small-scale data processing agents are defined as: microenterprises, small enterprises, startups, private legal entities, including non-profit entities, according to current legislation, as well as natural persons and depersonalized private entities that carry out personal data processing, assuming typical obligations of a Controller or Processor (Resolution CD/ANPD No. 2/2022, art. 2, I).

Microenterprises and small enterprises, according to Resolution CD/ANPD No. 2/2022, art. 2, II, are: business corporations, simple partnerships, single-member limited liability companies, and the entrepreneur referred to in art. 966 of the Civil Code[1], including individual micro-entrepreneurs, duly registered in the Commercial Registry or the Civil Registry of Legal Entities, that fit under art. 3 and 18-A, §1 of Complementary Law 123/2006.

Startups, according to Resolution CD/ANPD No. 2/2022, art. 2, III, are business or corporate organizations, newly established or recently operating, the activities of which are characterized by innovation applied to business models or the products or services offered, which meet the criteria provided in Chapter II of Complementary Law 182/2021.

6. How is the incident report filed, in practical terms?

Through ANPD's SEI website.

7. What should be included in the incident report?

Under LGPD, the incident Report must include, at least:

> I - a description of the nature of the affected personal data;
> II - information about the involved data subjects;
> III - an indication of the technical and security measures used to protect the data, considering commercial and industrial secrets;
> IV - the risks related to the incident;

[1] Law No. 10,406, of 10 January 2002 (Civil Code), art. 966:
"Art. 966. A businessperson is defined as someone who professionally engages in organized economic activity for the production or circulation of goods or services.
Sole paragraph. A person who practices an intellectual profession of a scientific, literary, or artistic nature, even with the assistance of helpers or collaborators, is not considered a businessperson, unless the practice of the profession constitutes an enterprise element."

V - the reasons for the delay, in the event that the report has not been immediate; and
VI - the measures that have been or will be taken to reverse or mitigate the effects of the harm.

Resolution CD/ANPD 15/2024 (art. 9) brings the following elements that must be included in the **incident Report directed to ANPD**:

I - a description of the nature and category of the affected personal data;
II - the number of affected data subjects, specifying, when applicable, the number of children, adolescents, or elderly individuals;
III - the technical and security measures used to protect the data, considering commercial and industrial secrets;
IV - the risks related to the incident, identifying possible impacts on the data subjects;
V - the reasons for the delay, in the event that the report was not made within the deadline (3 business days or double for small-scale agents);
VI - the measures that have been or will be taken to reverse or mitigate the effects of the incident, when applicable;
VII - the date of the occurrence of the security incident, when possible, and the date of its knowledge by the Controller;
VIII - the contact information of the Data Protection Officer or the representative of the Controller;
IX - the identification of the Controller and, if applicable, a statement that it is a small-scale processing agent;
X - the identification of the Processor, when applicable;
XI - a description of the incident, including the main cause, if it can be identified; and
XII - the total number of data subjects whose data is processed in the activities affected by the incident.

Regarding the **Report of the incident to data subjects**, it must meet the following criteria, as stated in Resolution CD/ANPD 15/2024:

I - use **simple and easily understandable language**; and
II - occur in a **direct and individualized manner** (conducted through the means typically used by the Controller to contact the data subject, such as phone, email, electronic message, or letter), when it is possible to identify them.

In addition, it must contain:

I – the description of the nature and category of the affected personal data;
II - the technical and security measures used to protect the data, observing commercial and industrial secrets;
III - the risks related to the incident, identifying possible impacts on the data subjects;

IV - the reasons for the delay, in the event that the report was not made within the specified deadline;
V - the measures that have been or will be taken to reverse or mitigate the effects of the incident, when applicable;
VI - the date of knowledge of the security incident; and
VII - the contact details for obtaining further information and, when applicable, the contact details of the Data Protection Officer.

If direct and individualized communication is not feasible or it is not possible to identify the affected data subjects, in total or in part, the Controller must report the occurrence of the incident, within the deadline and with the information defined in art. 9 of Resolution CD/ANPD 15/2024, through available disclosure means, such as its website, applications, social media, and data subject service channels, in a manner that allows for broad knowledge, with direct and easy visibility, **for a minimum period of three months**.

The Controller must attach to the incident report process a statement that it has communicated with the data subjects, specifying the means of communication or disclosure used, in up to three business days from the end of the deadline for reporting to ANPD.

8. What are the consequences of the incident communication to the Controller?

ANPD will assess the **severity** of the incident and may determine that the Controller take **measures** such as (i) broad disclosure of the fact through communication channels; and (ii) actions to reverse or mitigate the effects of the incident, if the authority deems it necessary to safeguard the rights of the data subjects (LGPD, art. 48, § 2, I and II).

To evaluate the severity of the incident, any evidence that **appropriate technical measures** have been implemented to render the affected personal data unintelligible, within the scope and technical limits of their services, for unauthorized third parties will be assessed (LGPD, art. 48, § 3).

LGPD stipulates that the systems used to process personal data must be structured to meet: (i) security requirements, (ii) standards of good practices and governance, and (iii) general principles provided for under LGPD and other regulatory norms (LGPD, art. 49).

SOURCES

BRAZIL. **Law No. 13,709, of 14 August 2018**. General Data Protection Law (LGPD). Federal Official Gazette, Brasília, DF, 15 Aug 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Access on 23 August 2024.

BRAZIL. **Resolution CD/ANPD** No. **2, of 27 January 2022.** Approves the Regulation for the application of Law No. 13,709, of August 14, 2018, LGPD, for small-scale processing agents. Federal Official

Gazette, Brasília, DF, 28 Jan 2022. Available at: Resolution CD/ANPD 2/2022. Access on 23 August 2024.

BRAZIL. **Resolution CD/ANPD No. 15, of 24 April 2024.** Approves the Regulation on the Reporting of Security Incidents. Federal Official Gazette, Brasília, DF, 26 Apr 2024. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Access on 23 August 2024.

BRAZIL. **Law No. 10,741, of 1 October 2003**. Provides for the Statute of the Elderly and makes other provisions. Federal Official Gazette, Brasília, DF, 3 Oct 2003. Available at: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm. Access on 8 October 2024.

BRAZIL. **Law No. 8,069, of 13 July 1990**. Provides for the Statute of the Child and Adolescent and makes other provisions. Federal Official Gazette, Brasília, DF, 16 Jul 1990. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Access on 8 October 2024.

CHECKLIST FOR REPORTING OF DATA SECURITY INCIDENTS:
STEP-BY-STEP GUIDE FOR CONTROLLERS

Has a security incident occurred? Here is how to proceed:

1. Has the event violated the following properties of personal data?
   - ☐ confidentiality
   - ☐ integrity
   - ☐ availability
   - ☐ authenticity of security

   - ➢ If any of the options above were selected, please continue.
   - ➢ If no option was selected, no security incident occurred according to ANPD, and, therefore, reporting is not necessary.

Must the incident be reported?

2. Does the security incident significantly affect fundamental interests and rights of data subjects? For instance:

   - ☐ The processing activity impedes the exercise of rights or the use of a service
   - ☐ The event causes material or moral damage to individuals like in any one of the circumstances below:
     - ☐ Discrimination
     - ☐ Violation of physical integrity
     - ☐ Violation of the right to image and reputation
     - ☐ Financial fraud
     - ☐ Identity theft
   - ☐ Other circumstances affecting fundamental interests and rights of data subjects

3. Did the event involve any of the categories listed below?

   - ☐ Sensitive personal data
   - ☐ Data of children, adolescents, or elderly individuals
   - ☐ Financial data
   - ☐ Data for authentication in systems
   - ☐ Data protected by legal, judicial or professional confidentiality
   - ☐ Data in large scale

   - ➢ If no items were selected in items 2 and 3 above, it is not necessary to proceed or to report to ANPD and to data subjects.