Regulation on Reporting Security Incident

RESOLUTION CD/ANPD Nº 15
OF APRIL 24, 2024

ANPD

ANNEX

REGULATION ON REPORTING SECURITY INCIDENT

CHAPTER I

GENERAL PROVISIONS

Article 1. This Regulation aims to establish procedures for Reporting Security Incidents, which may entail risk or significant damage to data subjects, in accordance with art. 48 of Law No. 13,709, of August 14, 2018 - General Law on the Protection of Personal Data (LGPD).

Article 2. The objectives of this Regulation are:

I - to protect the rights of data subjects.

II - to ensure the adoption of the necessary measures to mitigate or reverse the effects of the damages caused;

III - to ensure the effectiveness of the principle of accountability by data processing agents.

IV - to promote the adoption of rules of good practices, governance, and appropriate prevention and security measures.

V - to foster a culture of personal data protection.

VI - to ensure that data processing agents act transparently and establish a relationship of trust with the data subject; and

VII - to provide support for the regulatory, supervisory and sanctioning activities of the National Data Protection Authority (ANPD).

CHAPTER II

DEFINITIONS

Article 3. For the purposes of this Regulation, the following definitions are adopted:

I - full disclosure of the incident in the media: a measure that may be determined by the ANPD to the controller, pursuant to Article 48, Paragraph 2, item I, of the Law No. 13,709, of August 14, 2018, within the scope of the security incident report process, such as publication on the controller's website, social networks or other media;

II - authenticity: the property by which it is ensured that the information was produced, issued, modified or destroyed by a specific natural person, equipment, system, body or entity.

III - category of personal data: classification of personal data according to the context of its use, such as personal identification data, system authentication data, financial data.

IV - report of a security incident: act of the controller that communicates to the ANPD and the data subject the occurrence of a security incident that may entail a risk or relevant damage to the data subjects.

V - confidentiality: the property by which it is ensured that personal data is not available or disclosed to unauthorized persons, companies, systems, agencies or entities.

VI – system authentication data : any personal data used as a credential to determine access to a system or to confirm a user's identification, such as login accounts, tokens and passwords.

VII - financial data: personal data related to the financial transactions of the holder, including for contracting services and purchasing products.

VIII - affected personal data: personal data whose confidentiality, integrity, availability or authenticity has been compromised in a security incident.

IX - data protected by legal or judicial secrecy: personal data whose secrecy arises from a legal norm or court decision.

X - data protected by professional secrecy: personal data whose secrecy arises from the exercise of a function, ministry, office or profession, and whose disclosure may cause harm to others.

XI - availability: the property by which it is ensured that personal data is accessible and usable, upon demand, by a natural person or a specific system, agency or entity duly authorized.

XII - security incident: any confirmed adverse event related to the violation of the confidentiality, integrity, availability and authenticity of personal data security.

XIII - integrity: the property by which it is ensured that personal data has not been modified or destroyed in an unauthorized or accidental manner.

XIV - security measures: technical and/or administrative measures adopted to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination.

XV - nature of personal data: classification of personal data as general or sensitive.

XVI - security incident investigation procedure: procedure instituted by the ANPD to investigate the occurrence of a security incident that has not been reported by the controller.

XVII - security incident report procedure: procedure instituted within the scope of the ANPD after receiving a security incident report .

XVIII - security incident notification process: administrative report process instituted within the scope of the ANPD that encompass both the investigation and notification procedures for security incidents; and

XIX - incident treatment report: document provided by the controller containing copies, in physical or digital form, of relevant data and information to describe the incident and the measures adopted to reverse or mitigate its effects.

CHAPTER III

SECURITY INCIDENT REPORTING

SECTION I

CRITERIA FOR REPORTING A SECURITY INCIDENT

Article 4. The controller shall notify the ANPD and the data subject of the occurrence of a security incident that may entail a risk or relevant damage to the data subjects.

Article 5. A security incident may entail significant risk or damage to data subjects when it may significantly affect the interests and fundamental rights of data subjects and, cumulatively, involves at least one of the following criteria:

I - sensitive personal data.

II - data of children, adolescents, or elderly people.

III - financial data;

IV - authentication data in systems;

V - data protected by legal, judicial or professional secrecy; or

VI - large-scale data.

Paragraph 1. A security incident that may significantly affect fundamental interests and fundamental rights will be characterized, among other situations, in those in which the processing activity may prevent the exercise of rights or the use of a service, as well as cause material or moral damages to the data subjects, such as discrimination, violation of physical integrity, or of the right to image and reputation, financial fraud or identity theft.

Paragraph 2. A large-scale data incident is one that involves a significant number of data subjects, also considering the volume of data involved, as well as the duration, frequency and geographic location of the data subjects.

Paragraph 3. ANPD shall publish guidelines with the aim of assisting data processing agents in assessing incidents that may entail risk or relevant damage to data subjects.

SECTION II

SECURITY INCIDENT REPORT TO ANPD

Article 6. The communication of a security incident to the ANPD shall be carried out by the controller within three working days, except where there is a deadline for communication provided for in specific legislation.

Paragraph 1. The period referred in the head provision of this article will be counted from the controller's knowledge that the incident affected personal data.

Paragraph 2. The security incident report shall contain the following information:

I - a description of the nature and category of affected personal data.

II - the number of data subjects affected, specifying, where applicable, the number of children, adolescents or elderly persons.

III - the technical and security measures used to protect personal data, complying with trade and industrial secrets.

IV - the risks related to the incident, identifying the possible impacts on the data subjects.

V - the reasons for delay, in cases in which communication was not made within the period provided for in the head of provision of this article.

VI - the measures that have been or shall be adopted to reverse or mitigate the effects of the incident on the data subjects.

VII - the date of the incident, when possible to determine it, and the date on which the controller became aware of it.

VIII - the details of the Data Protection Officer or of the person representing the controller.

IX - the identification of the controller and, if applicable, a statement that it is a small processing agent processing agent.

X - the identification of the operator, where 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 are processed in the processing activities affected by the incident.

Paragraph 3. The information may be supplemented, in a substantiated manner, within twenty working days, counting from the date of communication.

Paragraph 4. Reporting of security incidents shall be made via an electronic form made available by ANPD.

Paragraph 5. The reporting of a security incident shall be carried out by the controller, through the Data Protection Officer accompanied by a document proving the contractual, employment or functional relationship, or through an appointed representative, accompanied by a document with powers of representation before the ANPD.

Paragraph 6. The documents referred to in paragraph 5 of this article shall be presented together with the reporting of the security incident, within the period provided in the head provision of this article.

Paragraph 7. In the event of non-compliance with the provisions in paragraph 6 of this article, the ANPD may investigate the occurrence of a security incident through the security incident investigation procedure.

Paragraph 8. The terms set out in the head of provision of this article and in paragraph 3 of this article are doubled for small agents, in accordance with the provisions of the Regulation for the application of Law No. 13,709, of August 14, 2018, General Law on the Protection of Personal Data (LGPD), to small processing agents, approved by ANPD Board of Directors Resolution No. 2, of January 27, 2022.

Article 7. It is the controller's dutty to request the ANPD, in a justified manner, to keep confidential information protected by law, indicating those whose access should be restricted, such as those related to its business activity whose disclosure may represent a violation of commercial or industrial secrets.

Article 8. ANPD may request additional information from the controller, at any time, regarding the security incident, including the record of personal data processing operations affected by the incident, the data protection impact assessment (RIPD) and the incident processing report, establishing a deadline for sending the information.

SECTION III

COMMUNICATION OF SECURITY INCIDENT TO DATA SUBJECT

Article 9. The communication of a security incident to the data subject shall be carried out by the controller within three working days from the controller's awareness that the incident affected personal data, and shall contain the following information:

I - a description of the nature and category of affected personal data.

II - the technical and security measures used for data protection, complying with trade and industrial secrets.

III - the risks related to the incident, identifying the possible impacts on the data subjects.

IV -the reasons for delay, in cases in which communication was not made within the time limit set out in the head provision of this article.

V - the measures that have been or shall be adopted to reverse or mitigate the effects of the incident, where applicable.

VI - the date on which the security incident was discovered; and

VII - the contact details for obtaining information and, where applicable, the contact details of the Data Protection Officer.

Paragraph 1. The communication of the incident to data subjects shall meet the following criteria:

I - use plain and easy-to-understand language; and

II - be direct and individualized, if it is possible to identify them.

Paragraph 2. A communication carried out by the means usually used by the controller to contact the data subject, such as telephone, e-mail, electronic message or letter is considered to be direct and individualized.

Paragraph 3. If direct and individualized communication proves unfeasible or it is not possible to identify, partially or fully, the affected data subjects, the controller must communicate the occurrence of the incident, within the time period and with the information defined in the head provision of this article, through the available means of disclosure, such as its website, applications, social media and data subject service channels, so that the communication allows broad knowledge, with direct and easy viewing, for a period of at least three months.

Paragraph 4. The controller must attach to the incident report process a statement that the communication was made to the data subjects, stating the means of communication or disclosure used, within three business days, counting from the end of the period referred to in the head of this article.

Paragraph 5. For the purposes of the provisions of Article 52, Paragraph 1, item IX, of Law No. 13,709, of August 14, 2018, it shall be considered good practice to include, in the communication to the data subject, recommendations capable of reversing or mitigating the effects of the incident.

Paragraph 6. The deadline set out in the head of this article is doubled for small agents, in accordance with the provisions of the Regulation for the application of Law No. 13,709, of August 14, 2018, General Law on the Protection of Personal Data (LGPD) to small processing agents, approved by ANPD Board of Directors Resolution No. 2, of January 27, 2022.

CHAPTER IV

SECURITY INCIDENT REGISTRATION

Article 10. The controller shall keep a record of the security incident, including that which was not communicated to the ANPD and the data subjects, for a minimum period of five years, counting from the date of registration, unless additional obligations are found that require a longer maintenance period.

Paragraph 1. The incident record shall contain, at a minimum:

I - the date the incident was known.

II - a general description of the circumstances in which the incident occurred.

III - the nature and category of affected data.

IV - the number of affected data subjects.

V - an assessment of the risk and possible damage to data subjects.

VI - measures to correct and mitigate the effects of the incident, where applicable.

VII - the form and content of the communication, if the incident has been communicated to the ANPD and the data subjects; and

VIII - the reasons for the lack of communication, where applicable.

Paragraph 2. The storage periods provided for in this article do not apply to the entities referred to in article 23 of the LGPD, provided the rules applicable to permanent storage documents in the specific temporality table or defined by the National Archives Council are observed.

CHAPTER V

SECURITY INCIDENT REPORT PROCESS

SECTION I

GENERAL PROVISIONS

Article 11. The purpose of the security incident reporting process is to monitor the actions related to the processing and response to the incident that may entail risk or relevant damage to data subjects, to safeguard the rights of data subjects.

Sole paragraph. The provisions of the Regulation of the Enforcement Process and the Administrative Sanctioning Process, approved by ANPD Board of Directors Resolution No. 01, of October 28, 2021, apply to the security incident reporting process governed by this Regulation, where applicable.

Article 12. ANPD may carry out audits or inspections, at any time, with the processing agents, or determine their performance, to collect additional information or validate the information received, with the aim of supporting decisions within the scope of the security incident reporting process.

Article 13. The security incident reporting process begins:

I - ex officio, in the case of a security incident investigation procedure; or

II - upon receipt of the communication, duly formalized, in accordance with article 6, paragraph 5 of this Regulation, in the case of a security incident communication procedure.

Article 14. The security incident reporting processes may be analyzed in an aggregated manner, and any measures resulting from them may be adopted in a standardized manner, in accordance with the planning of the enforcement activity and the prioritization criteria defined in the Monitoring Cycle Report referred to in article 20 of the Regulation of the Enforcement Process and the Administrative Sanctioning Process within the scope of the National Data Protection Authority, approved by ANPD Board Resolution No. 1, of October 28, 2021.

Article 15. During the process of reporting a security incident, the ANPD may determine that the controller, with or without prior notice, immediately adopt the preventive measures necessary to safeguard the rights of data subjects, in order to prevent, mitigate or reverse the effects of the incident and avoid the occurrence of serious and irreparable damage or damage that is difficult to repair.

Sole paragraph. ANPD may set a daily fine to ensure compliance with the determination provided for in the head of this article, in accordance with the Regulation on Dosimetry and Application of Administrative Sanctions, approved by ANPD Board of Directors Resolution No. 4, of February 24, 2023.

SECTION II

SECURITY INCIDENT INVESTIGATION PROCEDURE

Article 16. ANPD may investigate, through the security incident investigation procedure, the occurrence of incidents that may entail risk or relevant damage to data subjects, not reported by the controller, of which it becomes aware.

Paragraph 1. ANPD may request information from the controller to determine the occurrence of the security incident.

Paragraph 2. ANPD will assess the occurrence of the incident using the criteria set out in Article 5 of this Regulation.

Article 17. If a security incident is confirmed, the ANPD will order the controller to send the communication to the Authority and the data subjects, observing the deadlines and conditions described in articles 6 and 9 of this Regulation, respectively.

Paragraph 1. ANPD may also initiate an administrative sanctioning process to investigate non-compliance with the provisions of articles 6 and article 9 of this Regulation.

Paragraph 2. Once the security incident has been reported, as set out in the head of provision of this article, the security incident reporting procedure established in Section III will apply.

SECTION III

SECURITY INCIDENT REPORTING PROCEDURE

Article 18. The security incident reporting procedure will begin upon receipt of the incident report by the ANPD, duly formalized, in accordance with article 6, paragraph 5 of this Regulation.

Sole paragraph. Reports of the incident will be received exclusively through a specific channel, as per the guidelines published on the ANPD website.

Article 19. After assessing the severity of the security incident, the ANPD may order the controller to adopt measures to safeguard the data subjects' rights, such as:

I - full disclosure of the incident in the media; and

II - measures to reverse or mitigate the effects of the incident.

Paragraph 1. The severity of the incident will be assessed based on the information obtained and the criteria set out in Article 5 of this Regulation.

Paragraph 2. The measures mentioned in the head of this article shall be directly related to the incident.

Paragraph 3. ANPD may determine full disclosure of the incident in the media, at the expense of the controller, to safeguard the rights of data subjects, pursuant to article 48, paragraph 2, item I, of the LGPD, when the communication carried out by the controller proves insufficient to reach a significant portion of the data subjects affected by the incident.

Paragraph 4. The full disclosure of the incident in the media shall be compatible with the scope of the controller's activities and the location of the data subjects affected by the incident.

Paragraph 5. The incident may be fully disclosed in physical or digital media, always considering the need to reach the largest possible number of affected data subjects, with the following means of dissemination being permitted:

I - printed written media.

II - broadcasting of sounds and of sounds and images; or

III - transmission of information via the Internet.

Paragraph 6. The fully disclosure of the incident should not be confused with the sanction of public disclosure of the infraction referred to in article 52, item IV, of LGPD.

Paragraph 7. When determining the measures to reverse or mitigate the effects of the incident, it shall be considered those that can guarantee the confidentiality, integrity, availability and authenticity of the affected personal, as well as minimize the effects resulting from the incident for the data subjects.

Article 20. As an active transparency measure, ANPD may disclose, on its website, aggregated statistical information related to security incidents.

Article 21. ANPD may institute administrative sanctioning proceedings if the controller fails to adopt measures to reverse or mitigate the effects of the security incident within the timeframe and under the conditions determined by the Authority.

Article 22. The measures described in article 19 of this Regulation do not constitute sanctions for the regulated agent, and are equivalent to measures arising from preventive activity, under the terms of the Regulation of the Enforcement Process and the Administrative Sanctioning Process within the scope of the National Data Protection Authority, approved by ANPD Board Resolution No. 1, of October 28, 2021.

SECTION IV

TERMINATION OF THE SECURITY INCIDENT REPORTING PROCESS

Article 23. The security incident reporting process will be declared terminated in the following cases:

I - if no sufficient evidence of the occurrence of the incident is identified, subject to the possibility of reopening if new facts emerge.

II - if the ANPD considers that the incident does not have the potential to entail risk or relevant damage to the data subjects, in accordance with article 5 of this Regulation.

III - if the incident does not involve personal data.

IV - if all additional measures have been taken to mitigate or reverse the effects generated; or

V - the communication to the data subjects and the adoption of the relevant measures by the controller have occurred, in accordance with the LGPD, the provisions of this Regulation and the determinations of the ANPD.

Sole paragraph. In the case of item II of the head of this article, even with the declaration of termination of the security incident communication process, the ANPD may determine the adoption of security measures directly related to the incident, with the aim of safeguarding the data subjects' rights.

CHAPTER VI

FINAL PROVISIONS

Article 24. The provisions contained in this Regulation apply to the processes for reporting security incidents in progress when it comes into force, respecting the procedural acts which have already been carried out and consolidated.