CD/ANPD RESOLUTION No. 15 OF APRIL 24, 2024

Approves the Personal Data Breach Notification Regulation.

The Steering Committee of the NATIONAL DATA PROTECTION AUTHORITY (ANPD), exercising the powers conferred on it pursuant to article 5, I, of the Internal Rules of the National Data Protection Authority, as approved by Ordinance No. 1 of March 8, 2021, and according to the authority provided for in article 55-J, XIII, of Law No. 13,709 of August 14, 2018, in article 2, XIII, of Attachment I to Decree No. 10,474 of August 26, 2020, as well as the resolution taken in Proceeding No. 00261.000098/2021-67, has resolved as follows:

Article 1. The Data Breach Notification Regulation in the form of the attachment to this Resolution is hereby approved.

Article 2. Article 14, II of the Regulation on enforcement of Law No. 13,709 of August 14, 2018 - General Data Protection Act (LGPD) for small-sized processing agents, as approved by CD/ANPD Resolution No. 2 of January 27, 2022, becomes effective as follows:

"Article14 .....

II – to notify ANPD and the data subject of the occurrence of the data breach that may result in material risk or damage to data subjects, as set forth on the Data Breach Notification Regulation, approved by CD/ANPD Resolution No. 15 of April 24, 2024;

....." (NR)

Article 3. This Resolution comes into force on the date of its publication.

WALDEMAR GONÇALVES ORTUNHO JUNIOR
Chief Officer

ATTACHMENT

DATA BREACH NOTIFICATION REGULATION

CHAPTER I

PRELIMINARY PROVISIONS

Article 1. This Regulation is designed to regulate the process for notification of personal data breaches that are likely to result in material risk or damage to data subjects, pursuant to article 48 of Law No. 13,709 of August 14, 2018 - General Data Protection Act (LGPD).

Article 2. This Regulation has the following purposes:

I. to protect data subject rights;

II. to ensure the adoption of the requisite measures to mitigate or reverse the effects of the damage suffered;

III. to encourage compliance with the accountability principle [*princípio da responsabilização e da prestação de contas*] by processing agents;

IV. to promote the adoption of best practices and governance rules as well as adequate prevention and security measures;

V. to encourage the development of a personal data protection culture;

VI. to ensure that processing agents act in a transparent manner, and build a relationship of trust with data subjects; and

VII. to provide subsidies for ANPD's regulatory, supervisory, and sanctioning activities.

CHAPTER II
DEFINITIONS

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

I. full disclosure of the data breach in the media [*ampla divulgação do incidente em meios de comunicação*]: measure that may be determined by ANPD for the controller, pursuant to article 48, paragraph 2, I of the LGPD, within the context of the process for notification of personal data breaches, such as publication on the controller's website and social media or in other far-reaching media;

II. authenticity [*autenticidade*]: property designed to ensure that the personal data was produced, issued, modified or destroyed by a particular natural person, equipment, system, body, or entity;

III. category of personal data [*categoria de dados pessoais*]: classification of the personal data according to the context of their use, such as for personal identification, system authentication, and financial identification purposes;

IV. personal data breach notification [*comunicação do incidente de segurança*]: an act of the controller that communicates to ANPD and to the data subject the occurrence of a personal data breach that is likely to result in material risk or damage to data subjects;

V. confidentiality [*confidencialidade*]: property designed to ensure that the personal data will not be made available or disclosed to unauthorized or unaccredited persons, systems, bodies, or entities;

VI. system authentication data [*dado de autenticação em sistemas*]: any personal data used as a credential to determine access to a system or to confirm the identification of a user, such as login accounts, tokens, and passwords;

VII. financial data [*dado financeiro*]: personal data related to the data subject's financial transactions, including for contracting services and purchasing products;

VIII. affected personal data [*dado pessoal afetado*]: personal data whose confidentiality, integrity, availability or authenticity has been compromised in a data breach;

IX. personal data protected by legal or judicial secrecy [*dado protegido por sigilo legal ou judicial*]: personal data whose secrecy derives from a legal rule or court decision;

X. data protected by professional secrecy [*dado protegido por sigilo profissional*]: personal data whose secrecy derives from the exercise of a function, ministry, office or profession, and whose disclosure may cause harm to others;

XI. availability [*disponibilidade*]: property designed to ensure that the personal data will be accessible and usable, on demand, by a duly authorized natural person or a particular system, body or entity;

XII. data breach [*incidente de segurança*]: any confirmed adverse event related to the breach of properties such as confidentiality, integrity, availability and authenticity of personal data security;

XIII. integrity [*integridade*]: property designed to ensure that the personal data will not be subject to unauthorized or accidental alteration or destruction;

XIV. security measures [*medidas de segurança*]: technical and administrative measures adopted to protect personal data against unauthorized access and against accidental or unlawful destruction, loss, alteration, disclosure or dissemination;

XV. nature of the personal data [*natureza dos dados pessoais*]: classification of personal data into general or sensitive nature;

XVI. personal data breach investigation procedure [*procedimento de apuração de incidente de segurança*]: procedure carried out by ANPD to investigate the occurrence of a personal data breach that is likely to result in material risk or damage to data subjects and not notified by the controller;

XVII. personal data breach notification procedure [*procedimento de comunicação de incidente de segurança*]: procedure carried out within ANPD after receipt of a data breach notification;

XVIII. personal data breach notification proceeding [*processo de comunicação de incidente de segurança*]: administrative proceeding initiated within ANPD that encompasses the procedure to investigate the data breach and procedure to notify the data breach; and

XIX. data breach handling report [*relatório de tratamento de incidente*]: document provided by the controller containing copies, in physical or digital form, of relevant documents, data and information to describe the data breach and the actions taken to remedy it or mitigate its effects.

CHAPTER III
DATA BREACH NOTIFICATION
Section I
Data Breach Notification Criteria

Article 4. The controller shall notify ANPD and inform the data subject of the personal data breaches that are likely to result in material risk or damage to data subjects.

Article 5. A personal data breach is likely to result in material risk or damage to data subjects when it has the potential to significantly affect the fundamental rights and interests of data subjects, and involves, cumulatively, at least one of the following criteria:

I. sensitive data;

II. data of children, adolescents or elderly people;

III. financial data;

IV. system authentication data;

V. personal data protected by legal, judicial or professional secrecy; or

VI. large-scale data.

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

Paragraph 2. Large-scale data breaches shall be characterized as such when they involve a significant number of data subjects, also considering the volume of data involved, the breach duration and frequency, and the geographic extension of the location of the data subjects.

Paragraph 3. ANPD may publish guidelines aimed at assisting the processing agents in the evaluation of data breaches that are likely to result in material risk or damage to data subjects.

Section II
Notification of a Data Breach to ANPD

Article 6. The controller shall notify a personal data breach to ANPD within three business days, with due regard for the existence of another deadline set forth in specific legislation:

Paragraph 1. The deadline referred to in the main section of this article shall count as from the date the controller became aware of the personal data breach.

Paragraph 2. The data breach notification shall contain the following information:

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

II. the number of affected data subjects, specifying, where applicable, the number of children, teenagers or elderly people;

III. the technical and security measures for protection of personal data, adopted before and after the data breach, with due regard for trade and industrial secrets;

IV. the risks related to the data breach, along with identification of possible impacts on data subjects;

V. the reasons why the data breach had not been notified by the deadline set forth in the main section of this article;

VI. the measures that were or will be adopted to reverse or mitigate the effects of the data breach on the data subjects;

VII. the date on which the data breach occurred, where possible to determine it, and the date on which the controller became aware of it;

VIII. the information of the data protection officer [*encarregado*] or that of the person who presents the controller;

IX. the controller's identification data and, if applicable, a statement that it is a small-sized processing agent;

X. identification on the processor, when applicable;

XI. a description of the data breach, including the main cause, if identifiable; and

XII. the total number of data subjects whose data are processed in the processing activity affected by the data breach.

Paragraph 3. The information may be supplemented, in a circumstantiated manner, within twenty business days from the notification date.

Paragraph 4. The data breach must be notified through the electronic form made available by ANPD.

Paragraph 5. The notification of a data breach must be made by the controller, through the data protection officer, and it must be accompanied by a document proving the contractual, employment or functional link, or through a representative, accompanied by an instrument with powers of representation before the ANPD.

Paragraph 6. The documents referred to in paragraph 5 shall be provided along with the data breach notification, by the deadline set forth in this article.

Paragraph 7. In the event of infringement of the provisions in paragraph 6, the ANPD may investigate the occurrence of the data breach through a personal data breach investigation procedure.

Paragraph 8. The time period referred to in the main section and in paragraph 3 of this article is doubled for small-sized processing agents, in accordance with the provisions in the Regulation on enforcement of Law No. 13,709 of August 14, 2018 – General Data Protection Act (LGPD) for small-sized processing agents, as approved by CD/ANPD Resolution No. 2 of January 27, 2022.

Article 7. It is the controller's responsibility to request from ANPD, in a circumstantiated manner, the confidentiality of information protected by law, indicating the information whose access should be restricted, such as data on its business activity the disclosure of which may constitute a violation of trade or industrial secrets.

Article 8. ANPD may at any time request additional information from the controller regarding the data breach, including the record of the processing activities involving the personal data affected by the data breach, the data protection impact assessment (DPIA), and the data breach handling report, setting a deadline for submission of the information.

Section III
Communication of a Data Breach to Data Subjects

Article 9. The controller shall communicate a data breach to data subjects, within three business days after having become aware that the data breach has affected personal data, and the communication shall provide the following information:

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

II. the technical and security measures adopted to protect data, with due regard for trade and industrial secrets;

III. the risks related to the data breach, along with identification of the possible impacts on the data subjects;

IV. the reasons for delay, if the data breach has not been notified within the time limit set in the main section of this article;

V. the measures that were or will be adopted to reverse or mitigate the effects of the data breach, when applicable;

VI. the date on which the controller has become aware of the data breach; and

VII. the contact person to obtain information and, when applicable, the data protection officer's contact details.

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

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

II. to occur in a direct and individualized manner, if it is possible to identify the data subjects.

Paragraph 2. Direct and individualized communication is deemed to be that made through the means usually used by the controller to contact the data subject, such as telephone, e-mail, electronic message or letter.

Paragraph 3. If direct and individualized communication is not feasible or it is not possible to partially or fully determine the affected data subjects, the controller shall communicate the occurrence of the data breach, within the time limit and with the information defined in the main section of this article, through the available means of disclosure, such as its website, apps, social media and data subject service channels, so that the communication allows to become fully aware of it, with direct and easy viewing for a period of at least three months.

Paragraph 4. The controller shall attach to the data breach notification process a statement that a communication was made to the data subjects, containing the means of communication or disclosure used, within three business days from expiration of the time limit dealt with in the main section of this article.

Paragraph 5. Including recommendations capable of reducing the effects of the data breach in the communication to the data

subject may be considered good practice for the purpose of article 52, paragraph 1, IX of the LGPD.

Paragraph 6. The time limit in the main section of this article is doubled for small-sized processing agents, in accordance with the provisions of the Regulation on enforcement of Law No. 13,709 of August 14, 2018 (General Data Protection Act - LGPD) for small-sized processing agents, approved by CD/ANPD Resolution No. 2 of January 27, 2022.

CHAPTER IV
RECORDS OF DATA BREACHES

Article 10. The controller shall keep records of data breaches, including of those not reported to ANPD and data subjects, for at least five years from the date of the record, unless additional obligations are found to require a longer retention period.

Paragraph 1. The record of data breach shall contain at least:

I. the date on which the controller has become aware of the data breach;

II. a general description of the circumstances under which the data breach occurred;

III. the nature and category of affected data;

IV. the number of affected data subjects;

V. the risk assessment and possible damage to the data subjects;

VI. the measures to correct and mitigate the effects of the data breach, when applicable;

VII. the form and content of the communication, whether the data breach was reported to ANPD and the data subjects; and

VIII. the reasons for the lack of communication, when applicable.

Paragraph 2. The retention periods provided in this article do not apply to the entities set out in article 23 of the LGPD, as long as the rules applicable to permanent retention documents set forth in the document retention period chart [*tabela de temporalidade*] or defined by the National Archive Council [*Conselho Nacional de Arquivos*] are observed.

CHAPTER V
DATA BREACH NOTIFICATION PROCESS

Section I
General provisions

Article 11. The data breach notification process is designed to inspect acts related to the treatment and response of a data breach that may cause significant risk or damage to data subjects, in order to safeguard data subject rights.

Sole Paragraph The provisions in the Regulation on Inspection and Administrative Sanctioning Proceedings, approved by CD/ANPD Resolution No. 1 of October 28, 2021, apply to the data breach notification process governed by this Regulation.

Article 12. ANPD may, at any time, conduct audits or inspections at the processing agents, or determine their conduction, to collect additional information or validate the information received, with a view to supporting the decisions under the personal data breach notification process.

Article 13. A data breach notification process shall be commenced:

I. *ex officio*, in case of a data breach investigation procedure; or

II. upon receipt of a notification duly formalized pursuant to article 6, paragraph 5, in case of a data breach notification procedure.

Article 14. The data breach notification processes may be examined together and any measures arising thereform may be adopted in a standardized manner, in accordance with the planning of the inspection activity and the prioritization criteria defined in the Monitoring Cycle Report [*Relatório de Ciclo de Monitoramento*] dealt with in article 20 of the Regulation on Inspection and Administrative Sanctioning Proceedings within the National Data Protection Authority's sphere of authority, approved by Resolution No. 1 of October 28, 2021.

Article 15. In the course of the data breach notification process, ANPD may determine that the controller should adopt the necessary preventive measures to safeguard data subject rights, in order to prevent, mitigate or reverse the effects of the data breach and avoid the occurrence of a serious or hardly repairable damage, with or without the controller's prior answer.

Sole Paragraph ANPD may establish a daily fine to ensure compliance with the order set out in the main section of this article, pursuant to the Regulation on Calculation and Application of Administrative Sanctions, approved by CD/ANPD Resolution No. 4 of February 24, 2023.

Section II
Data Breach Investigation Procedure

Article 16. ANPD may investigate, under the personal data breach investigation procedure, the occurrence of personal data breaches that are likely to result in material risk or damage to data subjects which were not reported by the controller, of which it may have become aware.

Paragraph 1. ANPD may request that the controller provide information to determine whether a data breach has occurred.

Paragraph 2. ANPD shall assess the occurrence of a data breach according to the criteria set in article 5 of this Regulation.

Article 17. If the occurrence of a data breach is identified, ANPD shall determine that the controller should report the data breach to the Authority and the data subjects, within the time limits and under the conditions described in articles 6 and 9 of this Regulation, respectively.

Paragraph 1. ANPD may also commence administrative sanctioning proceedings in order to investigate the noncompliance set out in articles 6 and 9 of this Regulation.

Paragraph 2. After the data breach is reported pursuant to the main section of this article, the data breach notification procedure established in Section III shall apply.

Section III
Data Breach Notification Procedure

Article 18. The personal data breach notification procedure shall commence upon receipt of the data breach notification by ANPD, duly formalized, pursuant to article 6, paragraph 5.

Sole Paragraph The data breach notification shall be received exclusively through a specific channel, according to the guidelines published on ANPD's website.

Article 19. Once the severity of the data breach has been assessed, ANPD may determine that the controller should adopt the following measures to safeguard data subject rights, amongst others:

I. full disclosure of the personal data breach in the media; or

II. measures to reverse or mitigate the effects of the data breach.

Paragraph 1. The severity of the data breach shall be assessed based on the information obtained and the criteria dealt with in article 5 of this Regulation.

Paragraph 2. The measures referred to in the main section of this article shall be directly related to the data breach.

Paragraph 3. ANPD may determine full disclosure of the personal data breach in the media, to be afforded by the controller, in order to safeguard data subject rights, pursuant to article 48, paragraph 2, I of the LGPD, when the communication made by the controller is insufficient to reach a significant portion of the data subjects affected by the data breach.

Paragraph 4. The full disclosure of the personal data breach in the media shall be compatible with the scope of action of the data processing agent and the location of the data subjects affected by the data breach.

Paragraph 5. The data breach may be fully disclosed in physical or digital media, always considering the need to reach the greatest possible number of affected data subjects, with the following media being admitted, among others:

I. printed written media;

II. radio and television broadcasting; or

III. transmission of information via Internet.

Paragraph 6. Full disclosure of the data breach is not to be mixed up with the penalty of disclosure of the offense dealt with in article 52, IV of the LGPD.

Paragraph 7. On determining the measures to reverse or mitigate the effects of the data breach, ANPD shall consider those that may ensure the confidentiality, integrity, availability and authenticity of the affected personal data, as well as those that may minimize the effects arising from the data breach on the data subjects.

Article 20. As an active transparency measure, ANPD publishes aggregate statistical information on data breaches on its website.

Article 21. ANPD may commence administrative proceedings if the controller fails to adopt measures to reverse or mitigate the effects of the data breach within the time limit and under the conditions determined by the Authority.

Article 22. The measures described in article 19 of this Regulation do not constitute sanctions on the regulated agent, and are equivalent to the measures arising from the preventive activity, pursuant to the Regulation on Inspection and Sanctioning Administrative Proceedings within the National Data Protection Authority's sphere of authority, approved by CD/ANPD Resolution No. 1 of October 28, 2021.

Section IV
Termination of Data Breach Notification Process

Article 23. The personal data breach notification process may be declared terminated in the following cases:

I. if no sufficient evidence of the occurrence of the data breach is identified, subject to the possibility of reopening if new facts arise;

II. if ANPD considers that the data breach is not likely to result in material risk or damage to data subjects, pursuant to article 5 of this Regulation;

III. if the data breach does not involve personal data;

IV. if all additional measures to mitigate or reverse the effects produced have been adopted; or

V. if communication was made to the data subjects and the controller has adopted the relevant measures, in keeping with the LGPD, the provisions in this Regulation, and ANPD's resolutions.

Sole Paragraph In the event of item II of the main section of this article, even upon the declaration of termination of the data breach notification process, ANPD may determine the adoption of security measures to safeguard data subject rights.

CHAPTER VI
FINAL PROVISIONS

Article 24. The provisions contained in this Regulation shall apply to ongoing data breach notification processes, with due regard for the procedural acts already performed and consolidated.