02 de junho de 2023

Waldemar Gonçalves Ortunho Junior
Presidente, Conselho de Administração
Autoridade Nacional de Proteção de Dados

Re: ANPD - Regulation of Security Incident Reporting with Personal Data.

BSA | The Software Alliance appreciates the opportunity to provide the below comments in response to the National Agency of Data Protection (ANPD) draft resolution regarding the Regulation of Security Incident Reporting with Personal Data.

BSA is the leading advocate for the enterprise technology sector. Our members are among the world's most innovative companies and help to drive digital transformation by providing the solutions that make businesses and governments more competitive and effective, including cloud computing, customer relationship management, human resources management, identity and access management, data analytics, manufacturing, and infrastructure tools and services.

BSA shares your concern about the growing number of cyber incidents as well as their impacts on individuals, organizations, and the entire digital ecosystem. We endeavor to address those challenges through public-private collaboration. As we stated in Enhancing Cyber Policy, Advancing Digital Transformation: BSA'S 2023 Global Cyber Agenda, "In a world in which neither industry nor government alone can solve an ever-evolving set of challenges, public-private partnerships have proven to be the most effective approach to improving cybersecurity of both organizations and the digital ecosystem."

BSA applauds ANPD for noting in the draft regulation that the obligations to report relevant security breaches apply only to data controllers. This clarification provides legal certainty regarding the role of data processors, that should provide data controllers relevant information about security incidents, when applicable, but should not be held liable for the notification to ANPD and to the data subjects.

BSA offers the following specific comments.

1. **Security Incident Notification Criteria (Article 5)**

The draft regulation requires data controllers to notify ANPD when they are victims of security incidents that might create relevant risk or might cause relevant harm to data subjects. A security incident would meet this threshold if the security incident 1) has the potential to impact data subjects' fundamental rights and 2) fits in at least one of the categories listed in article 5.

Many incidents could be meet the first requirement mentioned above because many incidents could potentially impact data subjects' fundamental rights, which are defined broadly by article 5 § 1º as those that could prevent or limit access to a service or cause material or moral harm. Not all services are considered relevant enough to be deemed to have a relevant impact on a data subject's fundamental rights. Based on the current definition provided by article 5 § 1º, for example, if a data subject was unable to access a non-essential service for just a couple of minutes due to a security incident, the incident would be considered to have impacted a data subject's fundamental rights, which does not seem to support the thoughtful approach contained in the draft regulation. BSA recommends, therefore, that article 5 § 1º, I, be amended to include only incidents that impact essential services.

To further refine the scope, given the many incidents that would meet the requirement discussed in the previous paragraph (even with the improvement recommended by BSA), ANPD determined that an additional requirement would need to be present for an incident to be "relevant" for the purpose of notification. BSA recommends further refining the scope by ensuring that the categories of risk are aligned with the actual risks associated with a relevant security incident.

A. **Security incidents including data referring to children, adolescents, elderly people (article 5, II):** the level of risk of a security incident cannot be determined by the age of the data subject alone. For example, if two security incidents have the exact same characteristics, except that one of them includes data of 30 people who are between 25 and 40 years old and the second incident includes data of 29 people who are between 25 and 40 years old, and 1 person who is 70 years old, the level of risk associated with the two incidents may not be meaningfully different. In addition, for a data controller to know a data subject's age, the data controller would need to implement complex age-verification mechanisms that would result in collecting more data than necessary for the processing purposes, increasing privacy risks. BSA, therefore, recommends excluding article 5, II.
B. **Security incidents including system authentication data (article 5, IV):** Security incidents involving access to passwords that give access to a system do not necessarily create heightened risk to data subjects. For example, if a system requires a two or multiple factor authentication process, and only one set of the multiple factors has been compromised, then the result of the incident is not of the sort the ANPD is targeting because it would not create the type of risks that other incidents could create. Indeed, such a scenario demonstrates the value of implementing multifactor authentication. BSA recommends amending this provision to indicate that only incidents related to system authentication data that effectively provide access to those systems are within the scope of the requirement.
C. **Large amounts of data, (article 5, V):** The amount of data involved in a security incident does not determine its risk. For example, the risk associated with an incident including a large amount of data may be minimal or non-existent because it involved

only encrypted information. BSA recommends this item be excluded from the Draft Regulation.

2. **Notification Timeline (Article 6)**

The draft regulation requires a controller to notify ANPD within three working days of knowledge of the relevant security incident. While a three-day timeframe aligns with the laws of other leading countries like the Cyber Incident Reporting for Critical Infrastructure Act in the United States, an arbitrary deadline may not be conducive to ANPD or affected parties obtaining helpful information. Relatedly, for many security incidents of the type covered by the draft regulation, a data controller entity will not know with certainty the types of information ANPD seeks, for example the nature of the incident or the number of holders affected. In many circumstances, a data controller will know it is the victim of a security incident but will be working through its own response process to protect its users' data and determine information about the security incident.

A more flexible timeline for notification will help avoid overwhelming the ANPD with immaterial notifications and will prevent the diversion of company resources from response activities that improve security and privacy.

BSA recommends, that given the challenges of incident response, ANPD allow victim entities to report to ANPD within three working days or as soon as is practicable, which will increase the likelihood that a victim entity can obtain the information ANPD is requesting.

3. **Communication to the Holder (Article 9).**

The draft regulation requires data controllers to communicate the security incident to the data subject within three working days but provides no exceptions.

However, notifying data subjects in such short period of time may be counterproductive. For example, when such communication might exacerbate the risks to the data security and privacy of the data subject or interfere with an ANPD or other criminal investigation, notification should not be required.

In addition, data controllers may identify and respond to a relevant security incident and successfully avoid risks of harm to a data subject, in which case, the regulation should clarify that the data controller does not have the obligation to notify a data subject. For example, article 34 of the European Union's General Data Protection Regulation (GDPR) provides such exceptions.

BSA recommends ANPD include exceptions to the three-day communication requirement aimed at ensuring that any communication prioritizes the security and privacy of holders and does not undermine the purpose of the regulation.

4. **Data Retention (Article 10)**

The draft regulation requires data pertaining to security incidents, even to those incidents that are not considered significant enough to trigger the notification requirement, to be kept for 5 years. Requiring data controllers to retain data creates privacy and security risks. While, in some circumstances, those risks may be outweighed by other benefits, that is unlikely to be the case, particularly for situations in which an incident did not rise to the level to require notification. BSA recommends ANPD revisit its data retention requirements.

5. Audits and Inspections (Article 18)

The draft regulation allows ANPD to "at any time" inspect and collect information for a data controller. The draft regulation does not specify the scope of an inspection or what an inspection would entail. For example, Article 18 could be misinterpreted as allowing ANPD officials to have access to the data processing facilities, which would raise security and privacy concerns, particularly when the party subject to the inspection is an enterprise (business-to-business) company that processes data on behalf of multiple customers who are not implicated in the ANPD investigation.

BSA recommends ANPD include both procedural and substantive safeguards, limiting when and how the regulation would authorize ANPD to inspect data, and ensuring those inspections to do not create greater risks to the privacy and security of customer data.

Sincerely,

Antônio Eduardo Mendes da Silva
Country Manager, Brasil
BSA | The Software Alliance