March 22, 2021

Waldemar Gonçalves Ortunho Junior
President, Board of Directors
National Data Protection Authority

Re: ANPD Consultation 2/2021

BSA| The Software Alliance (BSA) welcomes the opportunity to provide preliminary feedback to the National Data Protection Authority (Autoridade Nacional de Proteção de Dados - ANPD) on the request for input regarding the regulation that will implement the provisions of the Brazilian Personal Data Protection Law (LGPD) that refer to the security incident notifications (ANPD Consultation 2/2021).

BSA supports data protection rules that are risk-based, technology neutral, and flexible. BSA members have a deep and long-standing commitment to protecting their customers' data across technologies and business models. We, therefore, we commend the ANPD for its efforts to develop regulations targeted at minimizing the risks of relevant security incidents, mitigating the impact of such incidents when they occur, and reducing the complexity of compliance with security incident notification to increase their effectiveness. We offer the answers to the questions posed in the Consultation 2/2021 document to contribute to ANPD's efforts to achieve these goals.

CONSULTATION QUESTIONS

1 - When can a security incident cause a significant risk or harm to the data subject? What criteria should be considered by the ANPD to classify the risk or damage as relevant?

A security incident should be deemed relevant for the purposes of trigging notification requirements when it creates a high of risk of identity theft or financial fraud.

2 - Should risk or damage be further classified into additional categories (e.g. low, medium, high, etc.)? How should the levels be distinguished from one another? Should low risk or damage be considered "relevant" or "not relevant"?

It is important that the regulation makes it clear that only relevant security incidents should trigger notification requirements, as the Brazilian Personal Data Protection Law (LGPD)

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

requires. To achieve this, the regulation needs to take a two-pronged approach: first, it is necessary define a security incident, and then offer guidance about when the security incident should be considered relevant to trigger the notification requirement.

Definition of Security Incident: Considering this Consultation relates to the implementation of the Brazilian Personal Data Protection Law (LGPD), the incidents within the scope of the upcoming implementing regulation should relate to personal data as defined by the LGPD. The regulation should make it clear that the security incidents requiring further analysis to determine if a security incident notification will be necessary are those that **negatively impact the privacy, availability or integrity of personal data** held by an organization.

Relevant Security Incident: Per the LGPD, only **relevant** security incidents should trigger the notification requirement. The **relevance** of a security incident should be assessed based on the likelihood that it will pose high risks of identity theft or financial fraud.

For instance, breach of personal data that is unusable, unreadable or indecipherable to an unauthorized third party due to the use of methods such as encryption, redaction, access controls and other mechanisms, should not trigger security notification requirements. Similarly, incidents affecting personal data that is already in the public domain are not likely to cause high risk of identity theft or financial fraud. For example, if a database listing only the names and professional affiliations of individuals whose publicly available social media profiles include these pieces of information were to be accessed by an unauthorized third party, this is incident would not be likely to create the risk of financial fraud or identity theft, and thus the incident should not be considered relevant for the purposes of this regulation.

3 - How should risk to the data subject and harm to the data subject be defined? How do these concepts relate to one another?

For the purposes of security incident notification, the **relevance** of the incident should be the determining factor. A security incident should be deemed relevant, trigging the notification requirement, if it poses a high risk of identity theft or financial fraud due to unauthorized access, destruction, use, modification, or disclosure of personal data.

According to the example referred to on the answer to question 2, if a databased listing only the names of individuals and their professional affiliations reflecting information that is publicly available were to be accessed by an unauthorized third party, the risk that this information will have a negative impact on those individuals due to financial fraud or identity theft is very low, so the incident would not be considered relevant. On the other hand, if the same database also contained data subjects' social security numbers, a risk that identity theft could occur would be present and the incident would then be considered relevant.

It is important the regulation makes it clear that notification will only be required if there are reasonable grounds to assume that a relevant security incident has occurred. Determining the occurrence of a relevant security incident requires an investigation by the data controller, so the mere fact that a company is made aware of a potential security incident should not trigger the notification requirement. Please see additional details on this issue on question 6 below.

4 - What elements should be considered when the risks of a security incident are assessed?

As described above, the potential for financial fraud or identity theft should be assessed when considering the risks posed by a security incident. This assessment can be made through a data protection impact assessment, for example.

5 - What pieces of information should the data treatment agents provide to the ANPD in addition to those already listed in art. 48, §1?
BSA notes for member reference only:
1) "data treatment agents" are defined by the law as data controllers and data processors, as applicable;
2) article 48 §1: The notification must take place within a reasonable timeframe, as defined by the National Authority, and shall contain, at the very least: I – a description of the nature of the affected personal data; II – information on the data subjects involved; III – an indication of the technical and security measures used to protect the data, without divulging trade secrets and proprietary information/methodologies; IV – the risks related to the incident; V – the reasons for delay, in cases in which the notification has not taken place immediate; and VI – the measures that were or will be adopted to reverse or mitigate the effects of the damage caused.

The information article 48, §1 requires is sufficient. If it is not possible to provide all the pieces of information required at the same time, the information may be provided in phases without undue further delay.

6 - What is a reasonable timeline for data treatment agents to inform the ANPD about a security incident? (art. 48, §1)

In the immediate aftermath of a security incident, companies should be encouraged - and afforded adequate time - to focus their resources on performing a thorough investigation and restoring the integrity of potentially compromised systems. Affording companies a reasonable timeframe for such efforts helps prevent additional damage.

Requiring notification in the first few hours after a company is made aware of a potential security incident forces the company to divert their resources from the incident investigation and from the implementation of actions that could mitigate or eliminate risk to data subjects. To ensure that companies act quickly upon learning of a potential security incident, the regulation should require that companies take immediate steps to establish whether there are reasonable grounds to assume that a relevant security incident has occurred. If after conducting this initial assessment the company concludes that a relevant security incident has occurred, it should take remedial actions to eliminate or reduce the likelihood of relevant harm to data subjects, as well as notify ANPD within 72 hours.

The deadline to notify the ANPD should start from the moment the company establishes with a reasonable degree of certainty that a relevant security incident has occurred and that it meets the notification threshold, and not when it first learns a potential security incident might have occurred. This approach will help avoid overwhelming the ANPD with immaterial notifications and will prevent the diversion of company resources from activities that foster

data security to the preparation of notifications that are unlikely to meet the notification threshold.

7 - What would be a reasonable timeline for data treatment agents to inform data subjects about the security incident (art. 48, §1)? What pieces of information should be included in this notification? Should the same pieces of information required by art. 48 , §1º be required?
Note for BSA member reference only: ***article 48 §1: The notification must take place within a reasonable timeframe, as defined by the National Authority, and shall contain, at the very least: I – a description of the nature of the affected personal data; II – information on the data subjects involved; III – an indication of the technical and security measures used to protect the data, without divulging trade secrets and proprietary information/methodologies; IV – the risks related to the incident; V – the reasons for delay, in cases in which the notification has not taken place immediate; and VI – the measures that were or will be adopted to reverse or mitigate the effects of the damage caused.***

Incident notifications should contain enough actionable information to allow data subjects to protect themselves from potential negative effects of a relevant security interest, without containing too many details that could render the notifications difficult to understand and ineffective.

The notification to data subjects should include the elements required by LGPD, art. 48 , §1º I, IV, and VI, as well as the name and contact details of the data protection officer or other contact point where additional information may be obtained. The notifying company may opt to add other pieces of information it deems relevant to a particular case.

Regarding timing for the notification, data subjects should be notified within a reasonable timeframe, which will vary depending on the circumstances. However, in cases when security incident notification to data subjects could negatively interfere with investigations being conducted by the ANPD and/or other legal authorities, and notification to data subjects could exacerbate the risks posed by the security incident, notification to data subjects should only be expected when the notifying company is cleared by the proper authorities to do so.

8 - What is the most appropriate way to communicate security incidents to data subjects? Should the notifications always be direct and individualized (by post, e-mail, etc.)? Or, public notifications should be allowed in certain circumstances (press release, internet postings, etc.)?

The notification methods should maximize the chances that the notification will reach the individuals affected by the security incident in a timely manner. Individual notification via postal mail, electronic mail, or telephone should be allowed for the cases in which those forms of communication are feasible. Companies should also be allowed to communicate with data subjects via their platforms if they consider this to be the best method to reach the data subjects impacted by the security incident.

Public notices, referred to as “substitute notice” by some US state laws, which are delivered through printed media or announcements prominently posted on the notifying company website should also be permitted when the notifying company does not have enough or up-to-date information for all the individuals impacted by the security incident. Public notices

should also be authorized if the notification is time-sensitive and individual notification would cause delays that could render the notification ineffective.

9 - What should be the exceptions to the obligation to inform the ANPD?

As the answer to question 2 above explains, only **relevant** security incidents should trigger the requirement to notify the ANPD. Notifications about other security incidents should not be required.

10 - What should be the exceptions to the obligation to inform the data subject?

When companies establish that there are reasonable grounds to assume that a relevant security incident might have occurred, they should take immediate remedial actions to mitigate or avoid the risk of harm to data subject. If remedial actions taken successfully eliminate risk to data subject, notification to data subjects should not be required. After reviewing the information received from the notifying company, if the ANPD is not satisfied that the remedial measures have been successful, it may require data subjects be notified.

For example, if credit information about various data subjects is removed from a database by an unauthorized third party posing risks to data subjects' credit scores, but the data controller is able to restore the data, the risk posed by the security incident would have been eliminated and notification to data subjects should not be required.

11 - What are the possible criteria to be adopted by the ANPD when analyzing the severity of the security incident? (art. 48, §2)
Note: the law says that depending on the severity of the incident the ANPD might require data controllers to take additional actions such as broad notifications through media and other means (in addition to notification to specific data subjects)

The higher the sensitivity and confidentiality of the data involved in a security incident, the more likely it will be that it may cause more severe harm due identity theft or financial fraud. For example, security incidents that cause the unauthorized access of individuals full names, addresses, drivers' license ("RG") and social security number ("CPF") are likely to trigger the notification requirement as this data is not normally broadly shared to prevent financial fraud and identity theft.

12 – Are there any recommended methodologies that should be used to assess the severity of security incidents? If so, which ones are recommended?

The ANPD could use international standards for information security such as ISO standards.

13 - What measures, including technical and administrative measures, could the ANPD require data treatment agents take after the security incident notification?

Because there is no such thing as perfect security, the risks of potential security incidents can never be entirely eliminated, but they can be mitigated and their effects can be stopped before harm to data subjects occur.

The ANPD should take a risk-based, technology neutral approach and require companies to maintain data security practices that are reasonably scoped to the size and complexity of an organization, the sensitive and volume of personal data on its systems, and he cos of available tools to improve security and reduce vulnerabilities.

14 – Are there any other suggestions you may wish to provide?

The role of data controllers and data processors

Security incident notifications to the ANPD and to the data subjects ("titular de dados"), when required, should be made by the company with whom data subjects have a direct relationship with (data controllers). This approach promotes good data stewardship, ensuring that data controllers take a lifecycle approach to managing information security.

Contracts between data controllers and its third-party data processors ("operadores de dados") should remain enforceable, allowing an efficient allocation of risk. In fact, to increase privacy protection, data processors often do not have visibility into what type of data they process, neither do they often have data subject's contact information. This would prevent data processors from making an accurate determination of whether the incident triggers notification requirements, and from reaching out to data subjects to notify them about the incident if needed.

If a security incident involving a data processor were to occur, the data processor must notify the data controller. The data controller would then assess the risk based on the information provided by the data processor and make a determination about the risk posed to data subjects by the incident, issuing the necessary notifications if they are warranted.