March 4, 2024

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

Re: ANPD Consultation on Data Subject Rights

BSA | The Software Alliance (BSA)[1] welcomes the opportunity to provide feedback to the National Data Protection Authority (Autoridade Nacional de Proteção de Dados - ANPD) on the public consultation for regulation on the rights of personal data owners under the Brazilian Personal Data Protection Law (LGPD).

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, cybersecurity, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

We recognize the importance of ensuring that individuals have rights over their personal data, including the right to access, correct, and delete that data. We commend the ANPD for conducting this consultation, which can help promote functional ways to implement these rights. Our comments focus on ensuring the new rights created by the LGPD work in practice.

I. Relationship Between Data Subject and Controller

The LGPD establishes important rights for data subjects. Importantly, data subjects must exercise the new rights created by LGPD through controllers, which are the companies that decide how and why to collect an individual's personal data. This structure is reflected in data

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

protection and privacy laws worldwide. BSA provides the following responses to the ANPD's initial questions about this relationship:

a. *Is it reasonable for the private sector to adopt deadlines like those provided for in Law No. 12,527 of November 18, 2011, to comply with the rights of the holder of personal data? If not, what would make it unfeasible to meet the deadlines and what would be reasonable?*

Controllers should be provided at least one month (30 days) to respond to any request by a data subject. Controllers should also be permitted extensions, such as allowing two further months for a response when appropriate. This timeframe aligns with the timeframes provided in other leading global data protection laws, including the European Union's General Data Protection Regulation (GDPR), which requires controllers to respond to data subject requests "without undue delay and in any event within one month of receipt," but permits controllers two-month extensions.[2] In Singapore, organizations are to respond to access requests "as soon as reasonably possible," but must inform an individual if they are unable to respond to an access request within 30 days.[3]

Aligning the LGPD's timeline for responding to data subject rights requests with timelines recognized in other global data protection laws can encourage companies to route Brazilian requests through established, regularly updated compliance practices, instead of requiring companies to create one-off approaches to handling Brazilian requests.

b. *When defining deadlines, what criteria should be considered to make differentiated provisions, as provided for in items I and II of the caput of art. 19 of the LGPD?*

Controllers should be permitted to identify the criteria for providing simplified notice under Article 19 of LGPD. This is important because controllers should draft a simplified notice differently for different types of products and services. In addition, companies will often need to review their records in order to determine if they are processing an individual's personal data. Although Article 19 states that controllers must respond to a data subject exercising her right to confirm the existence of or access to personal data "immediately" in a "simplified format," we encourage the ANPD to recognize this is not possible in all circumstances. For example, when a data subject is not a registered user or account holder with that controller, the controller may require time to review its records in order to confirm whether it is processing that individual's personal data. We encourage the ANPD to recognize these circumstances, by either not requiring companies to respond immediately or by recognizing that companies may satisfy this obligation by providing a simplified notice stating that they are reviewing their records in response to the data subject's request.

c. *What characteristics of a service channel are essential to ensure effective communication between the data subject and the processing agent?*

Data subjects should exercise rights under the LGPD by submitting a request directly to a controller. Controllers should be required to inform data subjects about specific ways in which they can exercise these rights, such as describing the process in the controller's privacy

[2] *See* EU General Data Protection Regulation Art. 12.3.
[3] *See* Singapore Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Sec. 15.18 (Revised May 16, 2022), *available at* https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-key-concepts/advisory-guidelines-on-key-concepts-in-the-pdpa-17-may-2022.pdf.

policy, which should be made public on the controller's website. It is important that the ANPD avoid creating overly specific requirements about the methods by which a data subject exercises these rights, because of the wide variety of controllers that must honor rights requests across a broad range of products and services. The best communication methods for exercising these rights will vary greatly across different products and services.

d. Are operators responsible for realizing the rights of holders? How should they cooperate with the controllers to fulfill the rights of the holders?

The LGPD recognizes the different roles of controllers (which decide how and why to collect a data subject's personal data) and operators (which process personal data on behalf of a controller and subject to its instructions). Because the controller is the company that decides to collect a data subject's personal data — and the company that decides how and why that data is processed — data subjects should exercise their rights under the LGPD by going directly to a controller. An operator, in turn, should be obligated to assist the controller in fulfilling a data subject right request by providing appropriate technical and organizational measures, insofar as possible.[4] But operators should not be required to respond directly to a data subject's request. This structure is in line with data protection and privacy laws worldwide.

There are strong privacy and security reasons for the ANPD to ensure data subjects exercise their rights by going to a controller, rather than an operator. For example, operators often do not review the personal data stored on their services — but may have to review data they otherwise would not if they were required to confirm if they are processing a particular individual's personal data. In addition, operators do not make the types of decisions required to respond to data subject rights requests, because responding to requests requires determining which data fields should be provided to a data subject, or whether information a data subject seeks to correct is inaccurate. Those decisions are made by controllers, as the entities that decide how and why to process an individual's personal data.

Indeed, the LGPD's text clearly provides that data subjects are to exercise new rights through a controller. Article 18, for example, creates new rights for data subjects "regarding the data subject's data being processed ***by the controller***" and clearly states that data subjects have the "right to obtain" certain information "***from the controller***." We strongly encourage the ANPD to recognize the importance of data subjects exercising rights by going directly to the controller.

e. Would it be feasible to adopt guidelines and procedures like those of the Consumer Service, established by Decree No. 11.034 of April 5, 2022, for exercising the rights of the holder of personal data? If not, which guidelines should not be adopted and for what reason?

Please see our comments above, in response to question c. It is important that the ANPD not take a one-size-fits-all approach to the method by which data subjects exercise rights under the LGPD, because those rights will apply to a variety of different products and services in which different methods may be appropriate.

[4] The obligation to provide "technical and organizational measures" is grounded in the EU's GDPR and adopted in more than a dozen state-level privacy and data protection laws in the United States. For more information about the role of processors in responding to data subject rights requests, please see BSA's document on Consumer Rights to Access, Correct, and Delete Data: A Processor's Role (explaining these issues in the context of US state privacy legislation), *available at* https://www.bsa.org/files/policy-filings/10122022controllerprorights.pdf.

f. Is there a service model adopted by private agents or the public sector that could serve as a paradigm, especially considering the ability to handle large volumes of demands economically? Give an example.

Please see our comments above, in response to question c. It is important that the ANPD not take a one-size-fits-all approach to the method by which data subjects exercise rights under the LGPD, because those rights will apply to a variety of different products and services in which different methods may be appropriate.

II. Right to Access

Article 18.I of the LGPD gives data subjects the right to obtain confirmation of the existence of the processing from a controller. Article 18.II of the LGPD similarly gives data subjects a right to obtain from a controller access to personal data processed by that controller. BSA provides the following responses about the application of these rights:

a. Is there an exceptional case for denying the right to confirm the existence of treatment? Give examples.

Yes, controllers should not be required to grant a data subject's access request in all cases. As an initial matter, this right should only apply if the controller has verified the data subject's identity, to avoid providing personal data to the wrong individual. In addition, there will be a range of circumstances in which granting access is not appropriate and the ANPD should recognize that controllers should not be required to provide access to personal data in such scenarios. These may include when providing access to personal data would restrict a controller or its operator's ability to:

- Comply with laws or regulations;
- Comply with a civil, criminal or regulatory inquiry from a government authority, or otherwise cooperate with law enforcement and regulatory agencies;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Provide a product or service specifically requested by a consumer;
- Perform a contract to which the consumer is a party, including fulfilling a written warranty;
- Take immediate steps to protect an interest that is essential for the life or physical safety of the data subject or another natural person;
- Prevent, detect, protect against, or respond to security incidents, identity theft, or any illegal activities, or preserve the integrity or security of their systems;
- Engage in public or peer-reviewed scientific or statistical research; or
- Assist another controller, processor, or third party, with any of these listed activities.

b. What information must be provided to data subjects to identify controllers, including in the case of shared use of personal data?

Data subjects should exercise their right of access by going to a controller directly. The controller should respond to the data subject based on the information available to that controller but should not be obligated to provide information related to or on behalf of another controller.

c. What is the responsibility of operators regarding the data subject's right to obtain information about the processing of personal data?

Please see our response to question I.d, above. As explained in that response, an operator should not be obligated to respond to data subject rights requests. Rather, controllers — the companies that decide how and why to process an individual's personal data — should be required to respond to such requests, as recognized in leading data protection laws worldwide. An operator, in turn, should be obligated to assist the controller in fulfilling a data subject right request by providing appropriate technical and organizational measures, insofar as possible.

d. What minimum information about the processing of personal data should be included in the declaration in simplified format provided for in Article 19, clause I, of the LGPD?

LGPD Articles 18 and 19 require controllers to confirm the existence of processing of personal data and to provide access to that personal data. Controllers should not be required to confirm the existence of processing in a specific manner, because this right applies to controllers that provide a wide range of products and services — and for which different forms of confirmation may be appropriate. We therefore recommend that the ANPD not require a "simplified format" notice to include a specific list of information, because of the potential for significant variation.

e. What minimum information about the processing of personal data should be disclosed by the controller, regardless of request - including the criteria and procedures used for the automated decision - to guarantee transparency and the right to information?

[BSA does not plan to respond to this question.]

f. Could the right of access be considered satisfied when the data controller makes the personal data available to the data subject in digital and paper format, as chosen by the data subject?

Yes. LGPD Articles 18 and 19 require controllers to provide access to the personal data of a data subject. This obligation should be considered fulfilled once access is provided.

III. Right to Data Portability

Article 18.V of the LGPD creates a right for data subjects to obtain from the controller the portability of their data to another service provider or product provider, by the means of an express request, pursuant with the regulations of the national authority and subject to commercial and industrial secrets. BSA provides the following responses about the application of this right:

a. In which sectors would the business processes and technology be mature enough to implement the right to data portability directly between processing agents, at the request of the data subject?

[BSA does not plan to respond to this question.]

b. What technological challenges must be faced to implement an interoperability standard?

[BSA does not plan to respond to this question.]

c. What aspects should be standardized to ensure interoperability (tools, format of portable data files, etc.)?

[BSA does not plan to respond to this question.]

d. Is it appropriate to consider the right to portability satisfied when the data controller makes all personal data available to the data subject in an interoperable format, as established in the regulation provided for in Art. 40 of the LGPD?

Yes. We encourage the ANPD to recognize that the right to portability may be satisfied by providing a data subject with the personal data that data subject previously provided to the controller in a portable, structured, and machine-readable format. This allows the data subject to transmit that personal data to another controller, without raising the security and privacy issues that may accompany requests to transmit personal data directly to another controller.

e. Is it reasonable to allow the private sector to define specific interoperability standards for certain economic activities for portability purposes? What timeframe would be reasonable?

[BSA does not plan to respond to this question.]

IV. Right to Correct Personal Data

Article 18.III of the LGPD provides data subjects the right to obtain from a controller the correction of incomplete, inaccurate, or out-of-data data. BSA provides the following responses about the application of this right:

a. What objective criteria should be considered to qualify a piece of data as incomplete, inaccurate, or out of date?

Controllers must exercise independent judgment to determine whether personal data is incomplete, inaccurate, or out of date. If a data subject believes a controller has inappropriately denied her request to correct personal data, however, the controller should have a clear process for data subjects to appeal such decisions.

b. In which situations would a simple declaration by the owner not be sufficient to exercise the right to correction? Please explain.

Controllers must exercise independent judgment in determining whether to honor a data subject's request to correct personal data. For instance, in some cases data subjects may seek to "correct" personal data that is accurate but unflattering; data subjects may also seek to "correct" data in ways that could create opportunities for fraud. If a data subject believes a controller has inappropriately denied her request to correct personal data, however, the

controller should have a clear process for data subjects to appeal such determinations.

c. What objective criteria should be considered to assess impossibility or disproportionate effort for the purposes of Art. 18, § 6 of the LGPD? Give an example.

There are a range of scenarios in which informing other processing agents about a data subject's exercise of consumer rights may be impossible or involve disproportionate effort, as recognized by LGPD Article 18 Section 6. Examples include when notification to other processing agents would require a controller to re-identify personal data that is stored in non-identifiable format, or would require the controller to collect personal data it would not otherwise collect. Both of these scenarios have the potential to create new privacy risks for data subjects, rather than increase data subjects' privacy. In addition, controllers should consider factors including the number of individuals involved, the age of personal data, and the safeguards adopted by the controller in determining whether an effort is disproportionate.

d. Is there an exceptional situation in which the right of correction can be denied by the controller? Give an example.

Yes, controllers should not be required to grant a data subject's correction request in all cases. As an initial matter, this right should only apply if the controller has verified the data subject's identity – to avoid correcting data that does not pertain to the data subject. In addition, there will be a range of circumstances in which correcting personal data is not appropriate. The ANPD should recognize that controllers should not be required to correct personal data such scenarios, including when providing access would restrict a controller or its operator's ability to:

- Comply with laws or regulations;
- Comply with a civil, criminal or regulatory inquiry from a government authority, or otherwise cooperate with law enforcement and regulatory agencies;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Provide a product or service specifically requested by a consumer;
- Perform a contract to which the consumer is a party, including fulfilling a written warranty;
- Take immediate steps to protect an interest that is essential for the life or physical safety of the data subject or another natural person;
- Prevent, detect, protect against, or respond to security incidents, identity theft, or any illegal activities, or preserve the integrity or security of their systems;
- Engage in public or peer-reviewed scientific or statistical research; or
- Assist another controller, processor, or third party, with any of these listed activities.

V. Anonymization, blocking, deletion, and opposition

Article 18.IV of the LGPD gives data subjects the right to obtain from the controller "anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of this Law." In addition, Article 18 Sec. 2 provides that a data subject may oppose the processing carried out based on a waiver of consent, if there is noncompliance with the LGPD. BSA provides the following responses about the application of these rights:

a. Is it necessary for the data subject to substantiate their request and prove that the data is unnecessary, that it is being processed excessively, or that it does not comply with the law? Give reasons.

[BSA does not plan to respond to this question]

b. Can anonymization and deletion be adopted alternatively, considering specific situations? Please explain.

[BSA does not plan to respond to this question]

c. Considering that the objection provided for in art. 18, § 2, of the LGPD would be applicable in the event of non-compliance with the provisions of the Law, what is its effect if the owner's claim is considered legitimate? Please explain.

[BSA does not plan to respond to this question]

VI. Right to Revoke Consent

Article 18.VI of the LGPD gives data subjects the right to request from a controller the deletion of personal data processed with the consent of the data subject, with limited exceptions. Article 18.IX of the LGPD gives data subjects the right to revoke consent, as provided in Article 8, Sec. 5. That provision, in turn, states that consent may be revoked at any time, by express request of the data subject, through a facilitated and free of charge procedure, with processing carried out under previously given consent remaining valid as long as there is no request for deletion. BSA provides the following responses about the application of these rights:

a. Does the revocation of consent provided for in art. 18, IX of the LGPD imply an obligation to delete personal data processed based on the data subject's consent? Please explain.

No. Individuals are given a range of rights under the LGPD and those rights should be exercised individually so that controllers can clearly understand an individual's request. In some cases, an individual may revoke her consent for a controller to process data in connection with a particular service. However, if the controller deletes that individual's data, it could prevent the controller from providing services for which the individual did not withdraw consent and would still like the controller to provide. This situation can be avoided if individuals exercise their new rights individually, so that controllers have clear instructions from a consumer about the right she intends to exercise.

b. Considering art. 8, what are the effects of the request for elimination on the treatments carried out under the protection of the consent previously expressed?

The LGPD gives data subjects the right to withdraw consent at any time. Importantly, Article 8 Sec. 5 recognizes that once consent is withdrawn, "processing carried out under previously given consent remain[s] valid as long as there is no request for deletion." We encourage the ANPD to recognize that: (1) the right to withdraw consent is forward-looking, and does not invalidate processing carried out under previously-given consent, and (2) that controllers must have reasonable notice of a data subject's intent to withdraw consent, so they can effectively implement it.

This approach would align with other leading global data protection laws. For example, under Singapore's Personal Data Protection Act, data subjects must give "reasonable notice" of their intent to withdraw consent. The Singapore Personal Data Protection Commission has recognized that there is no "one size-fits-all approach" to a specific timeframe for reasonable notice, but has said that notice of at least 10 days would be reasonable.[5] Similarly, the UK Information Commissioner's Office has recognized that if a data subject withdraws her consent "this does not affect the lawfulness of processing up to that point." While some controllers may be able to quickly implement a data subject's withdrawal of consent, the ICO recognizes that controllers may need a "short delay while [they] process the withdrawal."[6]

VII. Decisions Based on Automated Processing

Article 20 of the LGPD gives data subjects the right to request review of decisions based solely on automated processing of personal data affecting her or his interest, including decisions intended to define her/his personal, professional, consumer and credit profile, or aspects of her/his personality. Under this provision, the controller is to provide "clear and adequate" information regarding the criteria and procedures used for an automated decision, subject to commercial and industrial secrecy. If no information is provided under this provision, then the ANPD may carry out an audit to verify discriminatory aspects in automated processing of personal data. BSA provides the following responses about the application of these rights:

a. What would characterize an automated decision and a decision made solely based on automated processing of personal data? Please explain.

Automated decisions and decisions made solely based on automated processing of personal data should be regarded as those without human review or involvement in the decision-making process. This is consistent with guidance from leading data protection regulators. For example, the UK ICO has explained that "[f]or something to be solely automated there must be no human involvement in the decision-making process."[7] The Article 29 Working Party, in guidance later adopted by the European Data Protection Board, similarly explained that "[s]olely automated decision-making is the ability to make decisions by technological means

[5] *See* Singapore Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Sec. 12.40-41 (Revised May 16, 2022), *available at* https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-key-concepts/advisory-guidelines-on-key-concepts-in-the-pdpa-17-may-2022.pdf.
[6] UK Information Commissioner's Office, How Should We Obtain, Record, and Manage Consent, *available at* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent.
[7] *See* UK ICO, Rights Related to Automated Decision Making Including Profiling, *available at* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling.

without human involvement."[8]

b. What are the criteria for determining when an interest is being effectively affected? Explain.

The ANPD should create a clear standard for processing that "affects" an individual's interests and is therefore covered by this right. Other leading privacy laws do so by applying a right to decisions that produce legal effects about an individual. Under the GDPR, Article 22's right not to be subject to a decision based solely on automated profiling attaches if the processing "produces legal effects concerning him or her or similarly significantly affects him or her."

c. What are the practical challenges to implementing the right to review decisions provided for in Art. 20 of the LGPD?

The LGPD allows individuals to request "review" of decisions made solely based on automated processing. This provision appears to contemplate that a controller ask a human to review a decision, upon request of a controller. One issue that will arise as companies respond to such requests is handling a potentially large volume of requests. This problem would be exacerbated if the right applies broadly, such as if the ANPD adopts a broad standard for when a decision is deemed to "affect" an individual's interest. Conversely, adopting a narrower standard will decrease the number of decisions subject to this right, which may better position companies to provide human review upon request.

d. Are there situations in which the controller can deny the right to review automated decisions? Give reasons.

Yes, this right should not extend to processing that is necessary for a contract between the data subject and the controller, or processing based on the data subject's consent, or for processing authorized by other applicable legislation.

* * *

Thank you again for your focus on ensuring the rights provided to data subjects by the LGPD will function in practice. We welcome an opportunity to further engage with the ANPD on these important issues.

Sincerely,

Kate Goodloe
Managing Director, Policy
BSA | The Software Alliance

[8] *See* Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/697 (Oct. 3, 2017), *available at* https://ec.europa.eu/newsroom/article29/items/612053.