June 5, 2017

The Honorable Representative Orlando Silva
Brazilian House of Representatives
Praça dos Três Poderes
Brasília, DF CEP 70165-900

Re.: BSA Comments on Personal Data Protection Bill – PL 5276/2016

BSA| The Software Alliance[1] welcomes the opportunity to participate in the important dialogue on the future of data protection that is currently ongoing in Brazil. A balanced privacy regime that protects consumers without hampering innovation and the power of the digital economy will be very beneficial to the country.

As a global organization, BSA actively follows privacy developments around the world. BSA members have a deep and long-standing commitment to protecting consumers' personal data across technologies and business models as they recognize that consumers are only comfortable taking advantage of the benefits of new technologies if they trust that they will not lose control over their personal data.

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*

BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

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

We, therefore, commend and support the Brazilian Congress' efforts to create an overarching and balanced legal framework for the protection of personal data.

As the Special Committee further discusses PL 5276/2016, BSA appreciates the opportunity to share thoughts on the following topics to contribute to the improvement of the bill:

- Territorial Scope
- Definition of Personal Data
- Consent
- Other Basis for Data Treatment
- International Data Transfers
- Allocation of Liability and Responsibility
- Data Breach
- Time to Adoption

TERRITORIAL SCOPE:

The extensive use of the Internet, cloud-based services, the spread of the Internet of Things, and the ever-expanding data driven economy greatly complicates the application of the territoriality principle, since it can be nearly impossible to identify the exact location of an activity that happens online as occurring in a particular country.

BSA recommends that the Brazilian Personal Data Protection Bill apply to data treatment performed by an individual or legal entity, whether public or private, provided that : 1) Brazilian residents are specifically targeted, and 2) the personal data that is the object of the processing is purposefully collected within the national territory, refers to persons residing in Brazil at the time of the collection **and** such collection is performed by an entity established in Brazil or subject to Brazilian law by virtue of international public law .

Recommended Amendment [2]

Article 3 - *This Law applies to any treatment operation executed by a natural person or by a legal entity organized under public or private law, irrespectively of the country of its head office or the country where the data is located, provided that:*

I –The information collected specifically refers to a person that resides in Brazil ~~the treatment operation is executed in the national territory~~; and

~~II - the treatment activity is intended for the offering or the supply of goods or services or the treatment of data of individuals located in the national territory; or~~

III~~I~~ - the personal data object of the treatment is <u>purposefully</u> ~~was~~ collected in the national territory; and

<u>III – such collection is performed by an entity established in Brazil or subject to Brazilian law by virtue of international public law</u>.

~~Sole paragraph. The personal data shall be considered collected in the national territory when its owner [data subject] is there at the time of the collection.~~

<u>DEFINITION OF PERSONAL DATA</u>

We take note that applying very stringent legal obligations to a broad range of data, regardless of its context and the actual potential for harm to the user is likely to have a chilling effect on the data driven innovation in Brazil negatively impacting economic growth.

Therefore, we suggest that the legislation adopts a concept of personal data based on context, under which data would be deemed "personal data" only if it refers to a identified or identifiable natural person.

Recommended Amendment

Article 5 *– For the purposes of this Law:*

[2] Throughout this document, crossed out text indicates suggested deletions from original text of the Bill and highlighted text indicates suggested additions to original text of the Bill.

I. personal data: data related to identified or identifiable individual.~~, including based on identification numbers, location data or electronic identifiers when they are related to a person;~~

CONSENT

While we recognize that the data subject's consent can be a valid way of legitimizing the treatment of personal data, it should not be the only one. Other lawful basis for treating data should be considered equally valid.

Requiring consent as the primary way of legitimizing processing is problematic, as there may be instances in which obtaining consent may not be suitable or appropriate. For example, if a financial institution is collecting information on an outstanding debt and the institution needs to launch collection procedures, it may not be suitable to request the data owner's consent to do so but there is a legitimate business interest that would justify the collection (please refer to next section for more details on legitimate business interest).

Recommended Amendment

We applaud the changes that have already been incorporated to the Bill recognizing other ways to legitimize data treatment, including legitimate interest. This amendment should be maintained. In circumstances where consent may be necessary, it is important that the legislation focuses on the ends, not the means consent is provided. As long as consent is given freely, specifically and in an informed and unambiguous way, it should be accepted.

OTHER LAWFUL BASIS FOR TREATMENT:

The Brazilian Legislation should follow international best practices that accept a number of lawful basis for treating data in addition to consent.

Data treatment based on legitimate interest of the data controller should be authorized because it will allow new business based on data analytics to continue benefiting Brazilian citizens. Legitimate interest serves a particularly important role where it may not be suitable or appropriate for either the data controller to obtain consent to legitimize data collection and treatment or where it is premature to enter into a contract with a consumer. As long as the data subject's fundamental rights and freedoms are

respected, legitimate interest should be accepted as basis for data treatment.

Data treatment to ensure network and information security or to prevent fraud should also be allowed. Allowing data to be treated in these cases is important so that companies can protect their networks and the personal data entrusted on them by preventing unauthorized access, malicious code distribution, and stopping denial of service attacks.

Recommended Amendment

Article 7- *The treatment of personal data may only be carried out in the following cases:*

I - upon free, informed and unequivocal consent provided by the data subject;

II - for the fulfillment of a legal obligation by the responsible person[3];

III - by the public sector, for treatment and sharing of data necessary for the purposes of public policies established in laws or regulations;

IV - for the execution of historical, scientific or statistical research, guaranteeing, whenever possible, the anonymization of the personal data;

V - when necessary for the execution of an agreement or of preliminary procedures related to an agreement of which the owner is a party, at the data subject's request;

VI - for the regular exercise of rights linked to a judicial or administrative proceeding;

VII - for protection the life or of the physical well-being of the data subject or of a third party;

VIII - for the protection of health, with the procedure executed by health professionals or by sanitary entities;

IX - when necessary to meet the legitimate interests of the responsible person or of a third party, except in case of prevalence of the data subject's interests or fundamental rights and freedoms that demand the protection of the personal data, in special if the owner is underage.

X – when treatment is necessary for the purposes of ensuring network and information security or preventing fraud.

[3] "Responsible person" is the term used by the Bill for data controller

Article 10 *- The responsible person's legitimate interest may only be the grounds for treatment of personal data when reasonably necessary to support, deliver or improve services for the benefit of the owner, to carry out the responsible person's business functions or activities, or when consent is either impractical or unnecessary, ~~and based on a concrete situation,~~ respecting the owner's fundamental rights and freedoms.*

§ I- The legitimate interest shall contemplate the owner's legitimate expectations about the treatment of its data, according to the provisions of art. 6, item II.

§ 2- The responsible person shall take measures to guarantee the transparency of the treatment of data based on its legitimate interest~~, offering the data subject effective mechanisms to manifest his/her objection to the treatment of his/her personal data~~.

§ 3 When the treatment is based on the responsible person's legitimate interest, only the personal data strictly necessary for the intended purpose can be treated, being anonymized whenever compatible with the purpose of the treatment.

§ 4- The competent agency may request the manager to provide a privacy impact report when the treatment is based on its legitimate interest.

ALLOCATION OF LIABILITY AND RESPONSIBILITY

Relations between the operator (data processor) and responsible person (data controller), as well as assignor and assignee, should be governed by contracts or other legally binding acts, the breach of which would subject the parties to the provision of the civil code.

This clear allocation of responsibility and liability is critical and ensures that the increasingly wide-spread practice of outsourcing does not insert confusion in the system. This allocation allows the data subject and the legal authorities to know who to turn to in case of a problem, and companies have clarity on roles and responsibilities.

Direct, joint, and several liabilities on the operator / or the assignee would create a range of unintended consequences, undermining the relationship between the operator and the responsible person, creating an unjustified compliance burden. In addition, this could also have a negative impact on potential investments in data processing and outsourcing services in Brazil.

Data controllers ("responsible person") should have the primary obligation for ensuring compliance with applicable privacy law, while data processors ("operators") should be required to comply with data controller instructions and to ensure the security of the data they process.

Data controllers should have the primary obligation for ensuring compliance with applicable privacy law, while data processors should be required to comply with data controller instructions and to ensure the security of the data they process.

Recommended Amendment

Article 34 - *The authorization mentioned in item IV of the* ***introductory part of art.*** *33 shall be granted when the person responsible for the treatment presents sufficient guarantees of observance of the general principles of protection and of the data subject's rights by entering into ~~presented in~~ contractual clauses approved by the competent agency for a specific transfer, executing data transfer agreements ~~in~~ consistent with standard contractual clauses or ~~in~~ with global corporate standards or that include provisions that ensure compliance with this Law.*

§ 1- the competent agency may draft standard contractual clauses or homologate provisions contained in documents that set the grounds for the international data transfer, which shall observe the general principles of protection of data and of the owner's rights.~~, guaranteeing the joint and several liability of the assignee and of the assignor, irrespectively of fault~~.

§ ***2-*** *Those managers responsible for the treatment that are part of the same multinational economic group or conglomerate may submit global corporate standards for approval by the competent agency, mandatory for all companies that are part of the group or conglomerate, in order to obtain permission for the international transfers of data within the group or conglomerate without the need for specific authorizations, observing the general principles of protection and the owner's rights.*

§ 3 In the analysis of contractual clauses, documents or global corporate standards submitted for approval by the competent agency, supplementary information can be requested or verifications made about the treatment operations.

§ 4- The sufficient guarantees of observance of the general principles of protection of the owner's rights mentioned in the ***introductory part*** *shall also be analyzed according to the technical and organizational measures adopted by the operator, according to the provisions of § 1- and §* ***2-*** *of art. 45.*

Art. 35. T*he responsible person ~~assignor and the assignee~~ shall remain primarily responsible ~~be jointly and severally and objectively liable~~ for the data treatment and for providing redress to owners. Liability should be allocated among organizations responsible for the treatment according to their demonstrated fault giving raise to the liability. ~~irrespectively of the place where they are located, in any event.~~*

INTERNATIONAL TRANSFERS:

The ability to transfer data internationally is the lifeblood of the modern digital economy. Organizations transferring data must take appropriate steps to ensure user's information will be properly protected.

The "no transfer unless..." (adequacy) approach of the European legislation has been heavily criticized as it is at odds with the vast increase in global data flows that has occurred in the last 20 years, since its adoption.

We argue that the accountability model, first established by the OECD and subsequently endorsed and integrated in many legal systems and privacy principles, including the APEC Cross-Border Privacy Rules (CBPR) and Canada's Personal Information Protection Act (which received an adequacy determination from the EU), would provide an approach to cross-border data governance that effectively provides the individual with protections and fosters streamlined, robust data flows.

The accountability model requires organizations that collect data to be responsible for its protection no matter where or by whom it is processed would appropriately protect users. This approach requires organizations transferring data to take appropriate steps to ensure that any obligations – in law, guidance or commitments made in privacy policies – will be met.

We strongly encourage the Brazilian government to consider the benefits of allowing international transfers based on commitments assumed in international cooperation agreements, including international industry codes of conduct or frameworks developed through open, multi-stakeholder processes.

Furthermore, a system of mutual recognition for standard contractual provisions and global corporate standards should be put in place in order to avoid multiple and potentially contradictory global requirements.

Recommended Amendment

Art. 33. *The international transfer of personal data is only permitted in the following cases:*

I - to countries that provide a level of protection of personal data at least equivalent to that of this Law;

II - when the transfer is necessary for international judicial cooperation between public intelligence and investigation agencies, according to the international law instruments;

III - when the transfer is necessary for the protection of life or physical well-being of the owner or of a third party;

IV - when the competent agency authorizes the transfer;

V - when the transfer results from a commitment assumed in an international cooperation agreement, including international industry codes of conduct or international frameworks developed through open, multi-stakeholder processes;

VI - when the transfer is necessary for the execution of a public policy or legal attribution of the public service, making the publicity in the terms of art. 24; or

VII - when the owner has given its consent for the transfer, with previous and specific information about the international nature of the operation, with a warning about the risks involved.

Sole paragraph*. The level of data protection of the foreign nation shall be evaluated by the competent agency, which shall take into account:*

I - the general and sector specific rules of the legislation in effect in the destination country;
II - the nature of the data;
III - the observance of the general principles of protection of personal data established in this Law;
IV - the adoption of the security measures established in the regulation; and
V- the other specific circumstances relative to the transfer.

DATA BREACH

BSA supports the creation of a personal data breach notification system applicable to all businesses and organizations. Such a requirement could help incentivize entities to ensure robust protection for personal data, while enabling data subjects to take action to protect themselves in the event their data is compromised.

Any proposal should, however, be carefully crafted to prevent the issuance of immaterial notices, principally by ensuring that notice is only required where there is a serious risk of harm to the user. Furthermore, it should also exclude from the notice obligation all instances, where the lost data in question has been rendered unusable, unreadable or indecipherable to an unauthorized third party through practices or methods, which are widely accepted as effective industry practices or industry standards.

If a breach notification is required, it should occur in a reasonable timeframe, taking into account the time required to evaluate the nature and scope of the breach and whether the breach is likely to cause significant harm to data subjects.

Recommended Amendment

Article 47 - *The manager shall communicate to the competent agency the occurrence of ~~any~~ serious security incidents that could cause a significant harm ~~relevant risk or loss~~ to the owners.*

Sole paragraph. The communication shall be made in a reasonable time, as defined by the competent agency, taking into account the time required to evaluate the nature and scope of the breach and whether the breach is likely to cause significant harm to data subjects, and it shall mention at least:

I - the description of the nature of the personal data affected;
II - information about the owners involved;
III - the indication of the security measures utilized for data protection, including encryption procedures;
IV - the risks related to the incident;
V - the motives of the delay, if the communication was not immediate; and
VI - the measures that were or that shall be adopted to reverse or mitigate the effects of the loss.

TIME TO ADOPTION

Due to the complexity of the obligations set out in the new legislation, it is suggested that the rules provide companies with a period of adaptation of no less than two years.

Recommended Amendment

Article 56 - *This Law comes into effect ~~one hundred and eighty days~~ two years after the date of its publication.*

Sole paragraph. The competent agency shall establish rules on the progressive adaptation of databases constituted up to the date when this Law come comes into effect, considering the complexity of the treatment operations and the nature of the data.

We would like to once again thank you for the opportunity to participate in this dialogue that we hope will contribute to the creation of balanced public policies which will allow further innovation and economic growth spurred by the digital economy to occur Brazil.

We look forward to continue participating in this important discussion and stand ready to answer any questions you may have.

Sincerely,

Leticia S. Lewis
Director, Policy
BSA|The Software Alliance