



## **THE BUSINESS SOFTWARE ALLIANCE POSITION ON PRIVACY AND DATA PROTECTION**

The Business Software Alliance (“BSA”) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world’s commercial software industry and its hardware partners before governments and in the international marketplace.

BSA believes that the protection of personal information, and the prevention of information misuse that is very likely to cause harm, is important to fostering trust and confidence in the online experience and essential to the full development of the range of products and services that consumers will be willing to use and buy.

As a starting point, it may be useful for governments to consider instituting a legislative or regulatory framework that will provide overall guidance for businesses and consumers in relation to the principles of data privacy and protection. This is already the case in other jurisdictions around the world where there exists a comprehensive all-encompassing data protection framework or sector-specific legislation addressing the way personal information is collected and processed. Such governmental action will complement other mechanisms such as technology solutions, industry best practices, and consumer education to bring about a safer online environment. BSA believes such a framework should be consistent with the OECD Privacy Principles and the APEC Privacy Framework.

BSA believes that any legislation or regulation (including industry self-regulation guidelines) related to privacy and data protection should recognize, as did the APEC Framework, the economic value inherent in data processing in our increasingly information-based economies, and balance interests in individual privacy along with these and other important interests (e.g. public health measures). Also, BSA strongly supports the APEC Framework’s principle emphasizing the importance of protection against harm from misuse of personally identifiable information, and would recommend this objective as a central organizing principle of any national legislation or regulation.

BSA believes that any legislation or regulation that is adopted in relation to privacy and data protection should direct those who collect, store, process, use or disclose personally identifiable information (“PII”)<sup>1</sup> to provide to the individual:

- A clear and concise definition of what constitutes PII in a manner that is technology neutral.
- Notice – An individual should be informed about what PII will be collected, for which purpose(s), any third parties to whom it will be disclosed (excluding service providers and related companies operating under common policies), and the ways the individual can limit the use or disclosure of PII.

---

<sup>1</sup> PII refers to any information about an identified or identifiable individual.

- Collection – The collection of PII should be limited to that which is relevant to the stated purposes of collection and obtained by lawful and fair means.
- Use – PII should be used only to fulfill the stated or related purposes of the collection except with the consent of the individual whose PII was collected, when necessary to provide a service or product requested by the individual or under the authority of law. The PII collected should be proportionate to the purpose of the collection.
- Choice – Before PII is used for a different purpose or provided to a different party, the individual will be notified and consent obtained. Consent may occur in different ways (opt-in; opt-out<sup>2</sup>) and through different mechanisms (e.g. contract) depending on the circumstances.
- Integrity – PII should be reasonably accurate, complete and kept up-to-date for the intended use.
- Security – PII should be protected against risks such as loss or unauthorized access, unauthorized use, modification, disclosure, destruction or other misuses through reasonable administrative, technical and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities, and proportional to the likelihood and severity of the potential harm given the sensitivity of the PII and context in which it is held.
- Access/Correction – Individuals should be given reasonable access to PII pertaining to them for purposes of review and correction if erroneous and the ability to challenge denials of such requests.
- Accountability – An organization is responsible for PII under its control and should have a designated person(s) who is accountable for the organization's compliance with the above principles.

BSA believes that if a country is to adopt privacy or data protection legislation, in line with the APEC Privacy Principles, the legislation embodying the above principles should be flexible enough to take into account the great variety of business arrangements as well as the sensitivity of the PII and risks confronted within specific industry or market segments, while providing some consistency in the application of the rules across an economy and allowing for efficient cross-border implementations across different economies. The legislation also should not require the deployment or use of specific products or technologies, including any specific computer hardware or software, and permit various solutions and approaches to protect PII. The framework should provide for regulatory and contractual enforcement, rather than creating a general private right of action for damages.

---

<sup>2</sup> **Opt-in** refers to a requirement to seek the affirmative consent of an individual before using PII for a different purpose or providing it to a different party; **Opt-out** refers to the practice of informing individuals that their PII may be used for a different purpose or provided to a different party unless the individual notifies the entity with the PII that he or she objects.

## Data Breach

Finally, BSA notes that a number of countries have expressed interest in legislation that requires those who collect, store, process or use PII to notify individuals and/or regulatory authorities if they suffer a breach of their data security systems such that there is a significant risk of PII being used inappropriately, so that those individuals can evaluate the risk they face and take mitigation measures. BSA supports such legislation governing unauthorized access to or acquisition of PII, provided the legislation:

- Requires covered entities to develop, implement, maintain and enforce reasonable administrative, technical and physical safeguards, appropriate to the size and complexity of the entity, the nature and scope of its activities, and proportional to the likelihood and severity of the potential harm given the sensitivity of the PII and context in which it is held.
- Does not require the deployment or use of specific products or technologies, including any specific computer hardware or software, and permit various solutions and approaches to protect PII.
- Limits notification of data security breaches to those which present a significant risk of harm<sup>3</sup> to the individuals to whom the PII pertains, meaning that a reasonable person would conclude that there is a substantial likelihood that harm has occurred or will occur as a result of the breach, such as identity theft.
- Provides that notification is not required if the PII has been rendered unusable, unreadable or indecipherable to an unauthorized third party through the use of practices or methods such as encryption, redaction, access controls and other such mechanisms which are widely accepted as effective industry practices or an industry standard.
- Provides for government administrative enforcement and precludes private lawsuits for damages.
- Establishes a national law embodying these principles that is flexible enough to take into account the great variety of business arrangements as well as the risks confronted within specific industry or market segments.
- Prohibits the imposition of liability on an entity providing computer hardware, software or related services for the protection of PII in the event that the covered entity using those products or services was found to have violated the law's requirements.
- Prohibits the imposition of liability on a covered entity to a third party for damages resulting from a breach of security.

---

<sup>3</sup> Harm could occur, for instance, if the types of information involved in the breach such as unencrypted sensitive information is very likely to cause identity theft or financial loss.