GLOBAL PRIVACY BEST PRACTICES

BSA is the leading advocate for the global software industry, which is at the forefront of the development of cutting-edge innovation, including cloud computing, data analytics, and artificial intelligence. Software-enabled technologies increasingly rely on data and, in some cases, personal data, to function. As a result, the protection of personal data is an important priority for BSA members, and we recognize that it is a key part of building customer trust. To that end, BSA promotes a user-centric approach to privacy that provides consumers with mechanisms to control their personal data. BSA also supports data protection frameworks that ensure the use of personal data is consistent with consumers' expectations while also enabling companies to pursue legitimate business interests.

As countries around the world consider the development of data protection frameworks, many have sought to identify global best practices for approaching these issues. BSA supports the implementation of best practices that increase the transparency of personal data collection and use; enable and respect informed choices by providing governance over that collection and use; provide consumers with control over their personal data; provide robust security; and promote the use of data for legitimate business purposes. **We highlight below best practices that could help achieve these goals and serve as useful guideposts for the development and modification of data protection frameworks around the globe.**

ISSUE	BEST PRACTICE
Territorial Scope	Data protection frameworks should govern conduct that has a sufficiently close connection to the country. The law should apply where: (1) residents are specifically targeted; (2) the personal data that is the object of the processing is purposefully collected from data subjects in the country at the time of the collection; and (3) such collection is performed by an entity established in the country through a stable arrangement giving rise to a real and effective level of activity.
Definition of Personal Data	The scope of information included within the definition of personal data should be information that relates to an identified or identifiable consumer. An identifiable consumer is one who can be identified, directly or indirectly, through reasonable effort, by reference to an identifier such as an consumer's name, an identification number, location data, an online identifier, or one or more factors specific to the consumer's physical, physiological, or genetic identity of that consumer. The scope of information covered should pertain to personal data that, if mishandled, would have a meaningful impact on a consumer's privacy. Data that is de-identified through robust technical and organizational measures to reasonably reduce the risk of re-identification should not be covered data under the framework.

ISSUE	BEST PRACTICE
Harm	Data protection frameworks should tailor protections to the risk of harm to consumers. Cognizable harm should reflect physical injury, adverse health effect, financial loss, or disclosure of sensitive personal data that is outside the reasonable expectation of consumers and creates a significant likelihood of concrete adverse consequences.
Transparency	Data controllers should provide clear and accessible explanations of their practices for handling personal data, including the categories of personal data they collect, the type of third parties with whom they share data, and the description of processes the controller maintains to review, request changes to, request a copy of, or delete personal data.
Purpose Specification	Personal data should be relevant to the purposes for which it is collected and obtained by lawful means. Controllers should inform consumers of the purpose for which they are collecting personal data and should use that data in a manner that is consistent with that explanation, the context of the transaction, or reasonable expectation of the consumer, or in a manner that is otherwise compatible with the original purpose for which the data was collected. Controllers should employ governance systems that seek to ensure that personal data is used and shared in a manner that is compatible with the stated purposes.
Data Quality	Personal data should be relevant to the purpose for which it is used and, to the extent necessary for those purposes, should be accurate, complete, and current.
Grounds for Processing	Data protection frameworks should recognize and enable the processing of data for a range of valid reasons, including legitimate business purposes that are consistent with the context of the transaction or expectations of consumers. Other valid purposes include processing in connection with the performance of a contract; in the public interest or the vital interest of the consumer; necessary for compliance with a legal obligation; or based on the consumer's consent. Data protection frameworks should not restrict organizations' legitimate cybersecurity efforts; implementation of measures to detect or prevent fraud or identity theft; the ability to protect confidential information; or the exercise or defense of legal claims.
Consent	Controllers should enable consumers to make informed choices and, where practical and appropriate, the ability to opt out of the processing of their personal data. In settings where consent is appropriate, consent should be provided at a time and in a manner that is relevant to the context of the transaction or the organization's relationship with the consumer.
Processing Sensitive Personal Data	Certain data, such as financial account information or health condition, may be particularly sensitive. If the processing of sensitive data implicates heightened privacy risks, controllers should enable consumers from whom they collect sensitive data to provide affirmative express consent.

ISSUE	BEST PRACTICE
Consumer Control	Consumers should be able to request information about whether organizations have personal data relating to them and the nature of such data. They should be able to challenge the accuracy of that data and, as appropriate, have the data corrected or deleted. Consumers should also be able to obtain a copy of personal data that the consumer provided to the organization or was created by the consumer. Organizations should have the flexibility to determine the appropriate means and format of providing this information to the consumer. Controllers, which determine the means and purposes of processing personal data, should be primarily responsible for responding to these requests. Controllers may deny such requests where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the consumer's privacy; to comply with legal requirements; to ensure network security; to otherwise protect confidential commercial information; for research purposes; or to avoid violating the privacy, free speech, or other rights of other consumers. Controllers should also implement secure verification procedures to authenticate the consumer making the request to address the risk of harm of improper disclosure of information.
Security and Breach Notification	Controllers and processors should employ reasonable and appropriate security measures — relative to the volume and sensitivity of the data, size and complexity of the business, and cost of available tools — that are designed to prevent unauthorized access, destruction, use, modification, and disclosure of personal data. Data controllers should notify consumers as soon as practicable after discovering a personal data breach involving the unauthorized acquisition of unencrypted or unredacted personal data that creates a material risk of identity theft or financial fraud. Such breaches may be reported to supervisory authorities on a regular basis along with the security measures taken by the organization as part of accountability requirements.
Accountability Requirements	Controllers should develop policies and procedures that provide the safeguards outlined here, including designating persons to coordinate programs implementing these safeguards and providing employee training and management; regularly monitoring and assessing the implementation of those programs; and, where necessary, adjusting practices to address issues as they arise. As part of these measures, controllers may conduct periodic risk assessments when processing sensitive data and, where they identify a significant risk of harm, document the implementation of appropriate safeguards. Governments should not impose requirements to report risk assessments to or seek prior consultation with regulatory authorities, as they create unnecessary administrative burdens and delay the delivery of valuable services without a corresponding benefit to privacy protection.

ISSUE	BEST PRACTICE
Cross-Border Data Transfers	Data protection frameworks should enable and encourage global data flows, which underpin the global economy. Organizations that transfer data globally should implement procedures to ensure the data transferred outside of the country continues to be protected. Where differences exist among data protection regimes, governments should create tools to bridge those gaps in ways that both protect privacy and facilitate global data transfers. Data protection frameworks should prohibit data localization requirements for both the public and private sectors, which can frustrate efforts to implement security measures, impede business innovation, and limit services available to consumers.
Obligations of Controllers and Processors/ Allocation of Liability	Data controllers, which determine the means and purposes of processing personal data, should have primary responsibility for satisfying legal privacy and security obligations. Data processors, which process data on behalf of controllers, should be responsible for following the controller's instructions pursuant to their contractual agreements. Controllers and processors should have the flexibility to negotiate their own contractual terms, without mandatory, prescriptive language provided by the law.
Remedies and Penalties	A central regulator should have the tools and resources necessary to ensure effective enforcement. Remedies and penalties should be proportionate to the harm resulting from violations of data protection laws. Civil penalties should not be set arbitrarily or based on factors that lack a substantial connection to the context in which the underlying harm arose. Criminal penalties are not proportionate remedies for violation of data protection laws.