The Software Alliance

BSA

BSA PRIVACY FRAMEWORK

BSA is the leading advocate for the global software industry, which is at the forefront of developing 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 privacy frameworks that ensure the use of personal data is consistent with consumers' expectations while also enabling companies to pursue legitimate business interests.

Specifically, BSA supports legislation implementing 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. As set forth below, BSA outlines ten key components of privacy frameworks that help achieve these goals.

1 Transparency

Organizations 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 organization maintains to review, request changes to, request a copy of, or delete personal data.

2 Purpose Specification

Personal data should be relevant to the purposes for which it is collected and obtained by lawful means. Organizations should inform consumers of the purpose for which they are collecting personal data and 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. Organizations 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.

> BSA promotes a user-centric approach to privacy and supports privacy frameworks that ensure the use of personal data is consistent with consumers' expectations.

3 Informed Choice

Organizations should provide consumers with sufficient information to make informed choices and, where practical and appropriate, the ability to opt out of the processing of personal data.

BSA recognizes that certain data, such as financial account information or health condition, may be particularly sensitive. If the use of sensitive data implicates heightened privacy risks, organizations should enable consumers from whom they collect sensitive data to provide affirmative express consent.

Certain existing US laws, such as COPPA, HIPAA, GLB, and the FCRA, also provide important protections for the processing of sensitive personal data covered by those laws and should therefore remain in place.

more >>

4 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.

5 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 request a copy of the data, challenge the accuracy of that data, and, as appropriate, have the data corrected or deleted.

Organizations that determine the means and purposes of processing personal data should be primarily responsible for responding to these requests. Organizations 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.

6 Security

Organizations should employ reasonable and appropriate security measures designed to prevent unauthorized access, destruction, use, modification, and disclosure of personal data based on the volume and sensitivity of the data, size and complexity of the business, and cost of available tools.

7 Facilitating Data Use for Legitimate Business Interests

Privacy frameworks should facilitate the use of data for legitimate business purposes. Such purposes may include providing services to other business customers or consumers. Where the processing of data poses risks to the privacy of consumers, privacy frameworks should implement a risk-based approach that tailors protections to circumstances that are likely to lead to substantial harm.

8 Accountability

Organizations should develop policies and procedures that provide the safeguards outlined in this framework, including designating persons to coordinate programs implementing these safeguards and providing employee training and management; regularly monitor and assess the implementation of those programs; and, where necessary, adjust practices to address issues as they arise.

9 Legal Compliance and Enforcement

Organizations that determine the means and purposes of processing personal data should have primary responsibility for satisfying legal privacy and security obligations. Entities that process data on behalf of those organizations should be responsible for following their agreed upon instructions.

Any uniform federal privacy law should harmonize requirements in state law. The Federal Trade Commission, which has a strong record of robust enforcement, should have the tools and resources necessary to carry out its mission effectively.

10 International Interoperability

Privacy frameworks should enable and encourage global data flows, which underpin the global economy. Where differences exist among varying privacy regimes, governments should create tools to bridge those gaps in ways that both protect privacy and facilitate the free flow of data.