

BSA PERSONAL DATA PROTECTION PRINCIPLES

BSA | The Software Alliance (BSA) is the leading advocate for the global software industry before governments and in the international marketplace. Our member companies are at the forefront of data-driven innovation. BSA members have a deep and long-standing commitment to protecting consumers' personal data across technologies and business models. We recognize the importance of fostering trust and confidence in the online environment. As a global organization, BSA actively follows privacy developments around the world. An effective privacy regime protects consumers without hampering innovation and leverages the power of the digital economy to support governments and businesses alike.

BSA provides these Personal Data Protection Principles to advance the development of effective privacy and personal data protection regimes internationally. The Personal Data Protection Principles rest on five Pillars of Personal Data Protection.

PILLARS OF PERSONAL DATA PROTECTION

1. Scope and Definition of "Personal Data"
2. Collection, Use, Processing, and Disclosure of Personal Data
3. Allocation of Obligations and Liability
4. International Data Transfers
5. Personal Data Breach Notifications

1. Scope and Definition of "Personal Data"

PRINCIPLE


Definition of "Personal Data" should be reasonably linked to an identified or identifiable natural person.

RATIONALE

As any government seeks to protect individuals' personal data, it should also ensure that the scope of information included within the definition of personal data is information that, if mishandled, would have a meaningful effect on an individual's privacy.

If the scope is not limited, and stringent legal obligations apply to a broad range of data regardless of its context and the risk of harm to users, the law is likely to have a chilling effect on data-driven innovation, negatively affecting economic growth.

Any proposed legislation should also recognize that anonymized data, which is not linkable to a specific individual and, therefore, does not implicate privacy concerns, should be excluded from the definition of personal data.



According to international best practices, the legal bases for handling personal data could include, among other things, the legitimate interest of the data controller or third party, the consent of the data subject, compliance with legal obligations, and performance of a contract with the data subject.

2. Collection, Use, Processing, and Disclosure of Personal Data

PRINCIPLE

The legal bases for collecting, using, processing, and disclosing (collectively, “handling”) personal data should be sufficiently flexible so that they both ensure appropriate safeguards for personal data and allow businesses to continue to provide innovative services and stimulate economic growth.

RATIONALE

The legal framework for personal data protection should provide protections that meet, and are appropriate to, consumer expectations, without unnecessarily stifling economic growth through the data economy. According to international best practices, the legal bases for handling personal data could include, among other things, the legitimate interest of the data controller or third party, the consent of the data subject, compliance with legal obligations, and performance of a contract with the data subject.

Legitimate Interest

The legitimate interest legal basis for handling personal data would create the flexibility that companies need to carry out their business operations. For example, businesses may need to handle personal data as part of network security or fraud prevention efforts.

The legitimate interest legal basis also serves a particularly important role where it may not be suitable or practicable to obtain consent, or where it is premature to enter into a contract with the data subject. For example, if a financial institution is seeking to recover an outstanding debt and needs to collect, use, process, and/or disclose personal data as part of the debt-collection process (e.g., to debt-collecting agencies), it may not be suitable to request the data subject’s consent to do so, but there is a legitimate interest that would justify the handling of the personal data.

As long as the data subject’s fundamental rights and freedoms are respected, legitimate interest should be accepted as a valid basis for handling personal data.

Consent

Consent is another important basis for handling personal data. The standard for obtaining consent should be contextual to determine the level of consent that is appropriate.

In circumstances that do not implicate heightened sensitivity, implied consent may be appropriate. In today’s world, a large amount of data is created through individuals’ interactions with Internet-connected devices, and express consent is not suitable or practical in all instances. For example, the future of public transportation services may be affected if an individual must provide express consent to allow an electronic gate to generate data every time he or she swipes a public transportation card. In other circumstances, such as the handling of sensitive health or financial data, affirmative express consent may be appropriate. Any proposed legislation should consider this context and allow sufficient flexibility for determining the timing, standard, and mechanism for obtaining consent.


Relying solely on explicit written consent as a legal basis for handling personal data would create two risks: (1) stymying growth and innovation in the digital economy; and (2) not meeting consumer privacy expectations by leading consumers to “click fatigue,” where users simply accept whatever terms are presented to them without fully reviewing or understanding the information presented to them.

Compliance with Legal Obligations

Companies should also be able to handle personal data to comply with legal obligations. Businesses are subject to a wide range of legal obligations, including financial reporting rules, other regulatory requirements, and obligations arising from court proceedings. In some instances, companies must handle personal data to satisfy these legal obligations. Any privacy framework should ensure that companies can continue to comply with these requirements.

Contractual Performance

Similarly, companies should be able to handle personal data to perform contracts with the data subject. For example, a company may need to handle personal data to fulfill a product shipment ordered by an individual, or to open accounts at the request of the data subject.



The seamless transfer of data across international borders is critical to cloud computing, data analytics and other modern and emerging technologies and services. An effective personal data protection law should ensure that global data transfers continue.

Other Bases

In addition to the foregoing examples, there are several other potential circumstances that could serve as valid legal bases for handling personal data, including performance of tasks in the public interest and protecting the vital interests of data subjects. We recommend that governments adopt a flexible approach that both protects individuals' privacy and preserves companies' ability to carry out their legitimate business operations and provide innovative services to consumers.

3. Allocation of Obligations and Liability

PRINCIPLE

Responsibilities of "data controllers" and "data processors" should be clearly defined.

RATIONALE

The primary obligation for ensuring compliance with the applicable personal data protection law should fall on the "data controller." The "data processor" should only be concerned about complying with the instructions of the data controller, and to ensure the security of the data they process. The relationship between the data processor and data controller should be governed by contractual relationships they have formed.

This clear allocation of responsibility and liability is critical and ensures that the increasingly widespread 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 to have clarity on their roles and responsibilities.

Imposing direct, joint, or several liabilities or other obligations on data processors would have a range of unintended consequences, would undermine the relationship between these actors and would create an unjustified compliance burden. In addition, this could also have a negative effect on potential investments in data processing and outsourcing services.

In short, data controllers should have the primary obligation for ensuring compliance with applicable privacy law, whereas data processors should only be required through contractual mechanisms to comply with data controller instructions and to ensure the security of the data they process.

4. International Data Transfers

PRINCIPLE

The law should ensure the free flow of data across borders and avoid requirements that impose unnecessary or burdensome restrictions on global data transfers.

RATIONALE

The seamless transfer of data across international borders is critical to cloud computing, data analytics and other modern and emerging technologies and services that underpin the global economy. An effective personal data protection law should ensure that global data transfers continue.

The accountability model, first established by the OECD¹ and subsequently endorsed and integrated in many legal systems and privacy principles, provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data flows.

The accountability model requires organizations that collect personal data to be responsible for its protection, no matter where or by whom it is processed. As such, any organizations transferring personal data must take steps to ensure that any obligations — in law, guidance or commitments made in privacy policies — will be met.

International data transfers are often made with commitments assumed in international cooperation agreements — including international industry codes of conduct or frameworks developed through open, multi-stakeholder processes — which provide additional assurances that companies will appropriately safeguard personal data.

Furthermore, as part of ensuring the free flow of data, the law 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.

¹ *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe-protection-of-privacy-and-transborder-flows-of-personal-data.htm>.

5. Personal Data Breach Notifications

PRINCIPLE

Personal data breach notification requirements should be reasonable and appropriate and cover only situations where there is a material risk of harm to affected individuals.

RATIONALE

The creation of a personal data breach notification system applicable to all businesses and organizations would provide incentives to ensure robust protection for personal data, while enabling data subjects to take action to protect themselves in the event their data is compromised.

However, in creating such a system, it must be recognized that not all personal data breaches represent equal threats. In many instances, the breaches pose no actual risks to the individuals whose personal data was affected.

The notification requirements in the event of a personal data breach should therefore be carefully crafted to prevent the issuance of immaterial notices, principally by ensuring that notification is only required where there is a material risk of identity theft or economic loss to the user. Furthermore, it should also exclude from the notification obligation all instances where the personal data in question has been rendered unusable, unreadable, or indecipherable to an unauthorized third party through any practice or method that is widely accepted as effective industry practices or industry standards (e.g., encryption).

To ensure that data subjects receive meaningful notifications in the event of a personal data breach, it is also critical that data controllers and data processors are afforded adequate time to perform a thorough investigation to determine the scope and effect of the breach and prevent further disclosures. We recommend using a standard that is flexible such as "as soon as practicable" or "without undue delay" instead of specifying an arbitrary, fixed deadline for providing notification.



Data is now emerging as one of the most revolutionary forces for economic gains. We hope these Principles will assist governments worldwide in the development and implementation of effective personal data protection policies and privacy rules that protect consumers' personal data and also shape the growth of an emerging data-centric economy.

About BSA | The Software Alliance

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, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation and Workday.

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

+1.202.872.5500

@BSAnews

@BSATheSoftwareAlliance

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

+65.6292.2072

@BSAnewsAPAC

BSA Europe, Middle East & Africa

65 Petty France
Ground Floor
London, SW1H 9EU
United Kingdom

+44.207.340.6080

@BSAnewsEU