March 29, 2024

BSA COMMENTS ON THE DEVELOPMENT OF A LAW ON PERSONAL DATA PROTECTION

Respectfully to: The Ministry of Public Security

BSA | The Software Alliance (**BSA**)[1] thanks the Ministry of Public Security (**MPS**) for the opportunity to comment on the development of a Law on Personal Data Protection (**PDP Law**). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that spark the economy.

BSA has been actively participating in the developments related to personal data protection regulations in Vietnam. For instance, BSA provided comments on the draft PDP Decree in April 2021[2] and in June 2023.[3] BSA also attended the Workshop on the Cybersecurity Administrative Sanctions Decree organized by the MPS in November 2022, and actively participated in developments related to the Law on Cybersecurity and its various implementing decrees. Examples include BSA comments on Decree 53 in September 2022,[4] and BSA comments as on proposed amendments to the draft Decree 72 in September 2021[5] and December 2021.[6]

BSA commends the MPS for soliciting stakeholder input on the development of the PDP Law. This continues the positive practice of consulting with stakeholders, including industry, as you institute a national personal data protection regime. Putting in place a national personal data protection regime that is in line with global best practices is an important step in achieving the common goal of growing a vibrant and innovative domestic digital economy, while allowing Vietnamese companies to engage with the global digital economy. We recommend further active dialogue with the private sector and continued open discussions to achieve such common goals. These could include deeper collaboration between the MPS and other

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] BSA Comments on Draft Vietnam Personal Data Protection Decree, 09 April 2021 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-vietnam-personal-data-protection-decree.

[3] BSA Comments on the Personal Data Protection Decree No. 13/2023/ND-CP, 30 June 2023 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-superseding-decree-no-722013nd-cp.

[4] BSA Comments on Decree 53 to Implement the Law on Cybersecurity, 30 September 2022 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-decree-53-to-implement-the-law-on-cybersecurity.

[5] BSA Comments on Proposed Amendments to Draft Decree 72, 06 September 2021 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-proposed-amendments-to-draft-decree-72.

[6] BSA Comments on Proposed Amendments to Draft Decree 72 30 December 2021 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-proposed-amendments-to-draft-decree-72-0.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

government agencies with the private sector such as through roundtable discussions on how the PDP Law should be developed and subsequently implemented.

This submission to the MPS provides recommendations on the following areas:

- **Definitions of key terms**: Align definitions with those of international bodies, ensuring interoperability with key jurisdictions;
- **Roles and responsibilities of controllers and processors**: Ensure that roles and responsibilities of controllers and processors are clearly defined, including ensuring that the controller is responsible for responding to requests by the data subject;
- **Legal bases for processing personal data in addition to consent**: Recognize the processing of personal data for a broader range of independent bases, including processing necessary for legitimate interests, the performance of a contract, compliance with legal obligations, protecting the vital interests of the data subject, and the performance of tasks carried out in the public interest;
- **Cross-border transfers of personal data**: Adopt an accountability-based approach that recognizes a range of interoperable mechanisms such as contracts, binding corporate rules, and certifications; and only require data processing and cross-border transfer impact assessments to the data protection authority upon request;
- **Data breach notifications**: Limit obligations to notify the data subject or data protection authority only if a breach of personal data poses a high risk of material harm to the data subject;
- **Data subject rights**: Ensure that personal data controllers have sufficient time to respond to data subject requests, and align that timing with international best practices, i.e., 30 days; and
- **Transition period**: Include a two-year transition period for the implementation of the PDP Law, which would allow time for implementing regulations and guidelines to be issued and allow organizations sufficient time to adjust their systems and processes to comply with the PDP Law.

We hope that these suggestions will help the MPS to refine its reports: (1) The Report to Assess the Policy Impact of Developing a Law on Personal Data Protection (**Draft Policy Impact Report**), and (2) The Report to Assess the Current State of Social Relations Related to Personal Data Protection (**Draft Report on the State of Personal Data Protection**).[7] We hope to be a resource for MPS as you develop a comprehensive and robust PDP Law that is interoperable with international best practices, unifies Vietnam's data protection regulations, protects the legitimate rights and interests of organizations and data subjects alike, and supports the growth of a vibrant and innovative digital economy.

Definitions of Key Terms

BSA supports the intent within the Draft Policy Impact Report for the PDP Law to introduce key definitions,[8] including of the terms "personal data", "data subject", "personal data processing", "consent", "personal data controller", "personal data processor", and the "transfer of personal data abroad". It is important for the terms used in the PDP Law to align

[7] Public consultation documents in the draft dossier provided by the MPS, 01 March 2024 at https://bocongan.gov.vn/pbgdpl/van-ban-moi/du-thao-ho-so-de-nghi-xay-dung-luat-bao-ve-du-lieu-ca-nhan-t1282.html.

[8] Draft Policy Impact Report, paragraph III.1.4.2., pages 11-12.

with existing and emerging international best practices and regulations for personal data protection.[9]

Recommendation: The definition of such key terms should be aligned with definitions used by international bodies such as ASEAN in its Framework on Data Protection[10] and the OECD in its Privacy Framework.[11] The terms should also be interoperable with definitions in important jurisdictions such as the EU, Japan, and Singapore.

Roles and Responsibilities of Controllers and Processors

BSA strongly supports the Draft Policy Impact Report's recommendation to define personal data controllers and personal data processers.[12] The longstanding distinction between these two functions is foundational to privacy and data protection laws worldwide.[13]

Personal data controllers, which determine the means and purposes of processing personal data, should have primary responsibility for satisfying obligations around how and why personal data is collected and used. Personal data processors, which process data on behalf of controllers, should employ reasonable and appropriate security measures to prevents unauthorized access, use, or disclosure of personal data and should otherwise 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 that reflect these different roles.

While we support the recognition of the distinct roles of personal data controllers and personal data processors within the Personal Data Protection Decree No. 13/2023/ND-CP (**PDP Decree**), Article 39.4 in that Decree holds the personal data processor responsible to the data subject for damage caused by the processing of personal data. In practice, this creates tension between the data processor's role of supporting a data controller and the data controller's primary responsibility to the data subject. By definition, the personal data controller will determine how and why a data subject's personal information should be processed. The personal data processor, in turn, will handle that information on behalf of and at the direction of the personal data controller. As a result, the processor is following the controller's instructions and should not be held responsible for damage caused to the data subject by following those instructions. We recommend ensuring that the PDP Law does not conflate the responsibilities of these two roles and therefore does not hold data processors responsible for the responsibilities of data controllers, including the circumstances described above.

Recommendation: In contrast to the PDP Decree, the PDP Law should clarify that responsibilities to data subjects should be held by the personal data controller, which determines how and why to process a data subject's personal information. Personal data

---

[9] Draft Policy Impact Report, paragraph I.3., page 3.

[10] ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), Framework on Personal Data Protection, 25 November 2016 at https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

[11] OECD Privacy Principles, 11 July 2013 at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[12] Draft Policy Impact Report, paragraph III.1.4.2., pages 11-12.

[13] See BSA, Controllers and Processors: A Longstanding Distinction in Privacy, available in English and Vietnamese at https://www.bsa.org/policy-filings/the-global-standard-distinguishing-between-controllers-and-processors-in-privacy-legislation.

processors should continue to process personal data subject to reasonable and appropriate security measures and contractual safeguards to protect personal data. Personal data controllers and personal data processors should further define their distinct roles through contractual arrangements reflecting their different functions and capabilities.

Legal Bases for Processing Personal Data in Addition to Consent

BSA strongly supports the Draft Policy Impact Report's recommendation that there are legitimate reasons for processing personal data where the consent of the data subject is not required.[14] The PDP Law 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 transactions or expectations of data subjects. Other valid purposes include processing in connection with the performance of a contract; in the public interest or the vital interest of the data subject; necessary for compliance with a legal obligation; or based on the data subject's consent. The PDP Law should ensure the bases for processing data are drafted in a manner that does not restrict an organization's ability to utilize them independently or for legitimate cybersecurity efforts, the 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.

We encourage the MPS to adopt this approach to these issues in the PDP Law in contrast to the approach taken in the current PDP Decree. Under the PDP Decree, Articles 11 and 12 set out a consent-based personal data protection regime which requires individuals to review numerous consent requests for a wide range of processing activities. While Article 17 creates several exceptions to these consent requirements, such as protecting the life and health of individuals in an emergency, fulfilling contractual obligations, and reasons related to security and national defense, these exceptions are far narrower than those in many data protection laws adopted globally. As a result, companies doing business in Vietnam and consumers accessing products and services in Vietnam on the basis of the PDP Decree may be forced repeatedly to seek and provide consent, resulting in consent-fatigue, even for activities that may be reasonably expected by the consumer or are consistent with the initial purposes of processing.

Recommendation: The PDP Law should recognize that companies may process data without a data subject's consent for a range of activities. For instance, a company should be permitted to process personal data as necessary for purposes of legitimate interests it pursues, except when those interests are overridden by the rights and freedoms of a data subject. Globally, this ground for processing is often used in connection with activities including processing designed to prevent fraud, to improve the network and information security of a company's IT systems, or to improve the functionality of a product or service used by the data subject, among other pertinent activities in the usual course of business. Specifically, we recommend that the PDP Law recognizes the processing of personal data for legitimate interests if appropriate notice is provided and such processing does not adversely impact the rights and freedoms of the data subject. We also support recognizing a broader range of independent bases for processing beyond consent, including processing necessary for performance of a contract, processing necessary for compliance with legal obligations,

[14] See Draft Policy Impact Report, paragraph II.2.3., page 10; paragraph III.3.4.2. page 19; paragraph III.4.4.2. page 23.

processing necessary to protect the vital interests of the data subject, and processing necessary for the performance of tasks carried out in the public interest.

Cross-Border Transfers of Personal Data

BSA strongly supports the importance of facilitating cross-border transfers of personal data. We appreciate the acknowledgement in both the Draft Policy Impact Report and the Draft Report on the State of Personal Data Protection about the importance of international data transfers, for example in relation to Vietnam's commitments in international treaties and agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (**CPTPP**) and the European Union-Vietnam Free Trade Agreement (**EVFTA**).

The PDP Law should enable and encourage global data transfers, 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 not impose data localization requirements for either the public or private sectors, because such requirements can frustrate efforts to implement effective security measures, impede business innovation, and limit services available to consumers.

Recommendation: The PDP Law should adopt an accountability-based approach to support cross-border data transfers, under which the transferring organization remains accountable for ensuring that the receiving organization protects the transferred personal data to the same standards as those required under Vietnamese law. Additionally, the PDP Law should recognize a range of interoperable mechanisms for the cross-border transfer of personal data, such as contracts, including model contracts such as the ASEAN Model Contractual Clauses; intra-group schemes like binding corporate rules; and certifications like the Global and APEC Cross-Border Privacy Rules (**CBPR**) systems.

This approach would adopt an important change from the current PDP Decree which relies on consent to permit cross-border transfers of personal data. Furthermore, under the current PDP Decree, in addition to the data subject's consent each transfer requires: (1) a transfer impact assessment, and (2) reporting that transfer impact assessment to the MPS, with the requirement to submit updates and amendments accordingly. In practice, these provisions create significant barriers to cross-border data transfers.

As noted in our prior submissions, restrictions on cross-border transfers have a chilling effect on the local economy as they restrict domestic enterprises and other organizations from fully benefitting from cutting edge technology and services available in the global marketplace. For instance, restrictions on cross-border data transfers may prevent domestic companies, including small and medium-sized enterprises (**SMEs**) and larger organizations such as hospitals, airlines, and banks, from using world leading information technology and cloud computing solutions from service providers that offer their services from outside of Vietnam. Such services frequently provide best in class security capabilities. Domestic companies subject to data transfer restrictions are likely to find it difficult to access such services, reducing their competitiveness, especially internationally, and exposing them to greater data security risks. Restrictions on international data transfers are also resource-intensive for government authorities to manage. The additional impact assessment reporting obligations in the PDP Decree sap the resources of both the businesses seeking to conduct international commerce and the MPS, all with very little if any improvement in

the protection of personal information. Although we support privacy and security-protective regulations, the PDP Decree's onerous restrictions on cross-border data transfers undercut data protection and increase the risk that such data may be compromised by reducing access to privacy-protective and secure products and services.

Recommendation: We strongly recommend that the PDP Law be drafted to support international data transfers. Specifically, it should permit companies to transfer data internationally on legal bases not limited to the consent of the data subject and using mechanisms that do not require companies to conduct individual transfer impact assessments for each transfer. In addition, if data processing and cross-border transfer impact assessments are imposed for particular circumstances, they should be required to be submitted to the MPS or relevant data protection authority only upon request, as opposed to being required in every case. This would be consistent with international best practice and would help both companies and regulators better focus their resources on material instances.

Data Breach Notifications

BSA supports the creation of a personal data breach notification system applicable to all businesses and organizations. Appropriately crafted data breach provisions incentivize the adoption of robust data security practices and enable individuals to take action to protect themselves in the event their data is compromised. When developing data breach notification provisions, it is critical to recognize that not all data breaches represent equal threats. In many instances, an incident may pose no actual risks, particularly where prompt and reasonable efforts are taken, such that the personal data of individuals is not compromised. To ensure that data subjects and the data protection authorities are not inundated with notices regarding incidents that do not create significant risks of harm to the data subjects, the notification obligation should be triggered only if an incident poses a high risk of identity theft or financial fraud due to unauthorized access, destruction, use, modification, or disclosure of personal data. For instance, the obligation to provide notice should not apply to instances in which data is unusable, unreadable, or indecipherable to an unauthorized third party through practices or methods (e.g., encryption) that are widely accepted as effective industry practices or industry standards. Finally, to ensure users receive meaningful notification in the event of a breach, it is critical that data controllers are afforded adequate time to perform a thorough risk assessment to determine the scope of the security risk, prevent further disclosures, and determine the potential risks to data subjects as a result of the event. It is therefore counterproductive to include within the data breach provision a fixed deadline for providing notification.

Recommendation: We recommend including obligations to notify the data subject or data protection authorities only of a breach of personal data that poses a high risk of material harms, i.e., identity theft or financial fraud due to unauthorized access, destruction, use, modification, or disclosure of personal data. A personal data controller should not be required to provide any notification if there is not a high risk of material harm, including if the compromised data was stored in a manner that renders it unusable, unreadable, or indecipherable to an unauthorized third party through practices or methods that are widely accepted as effective industry practices or industry standards.

Data Subject Rights

BSA welcomes the proposed establishment of data subject rights for individuals within the Draft Policy Impact Report.[15] Data subjects should be made aware if organizations process personal data relating to them and the nature of such data and its use. Individuals should also be able to challenge the accuracy of that data and, as appropriate, have the data corrected or deleted. Data subjects should also be able to obtain a copy of personal data that they provided to the organization or was created by them.

As these rights are implemented, organizations should have the flexibility to determine the appropriate means and format of providing information to the data subject. Personal data controllers, which determine the means and purposes of processing personal data, should be primarily responsible for responding to these requests. Controllers should have the ability to deny such requests where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the data subject's rights; to comply with legal requirements; to ensure network security; to otherwise protect confidential commercial information; for research purposes; or to avoid violating the privacy and other rights and interests of other data subjects. Controllers should also implement secure verification procedures to authenticate the data subject making the request to address the risk of harm of improper disclosure of information.

We encourage the PDP Law to adopt an approach to data subject rights that can be practically implemented and in line with international best practices. Currently, PDP Decree Articles 14.3, 15.2, and 16.5 could be interpreted as requiring controllers to respond to certain data subject requests within 72 hours. As discussed in our previous submission,[16] such a short time frame imposes challenges such as verifying the identity of the requestor, clarifying the data subject's request, ensuring that the data subject understands the consequences of their request (such as in the case of a deletion request), and being able to manage high volumes of such requests. It is also out of step with leading data protection laws globally, which permit controllers at least 30 days to respond to data subject requests, with the potential for extensions.

Recommendation: Ensure that personal data controllers have sufficient flexibility and time to respond to data subject requests and align that flexibility and timing with international best practices, i.e., within 30 days. The EU General Data Protection Regulation (**GDPR**) allows controllers 30 days to respond to a data subject access request. Similarly, the Singapore Personal Data Protection Act (**PDPA**) also allows organizations 30 days to respond to an access request from a data subject.

Transition Period

As acknowledged in both the Draft Policy Impact Report and the Draft Report on the State of Personal Data Protection, there is currently little harmonization in the domestic laws and regulations addressing personal data protection in Vietnam. With the promulgation of a Personal Data Protection Law and the accompanying implementing regulations and guidance, we can expect many issues and challenges when implementing new data protection processes and practices. Government agencies, organizations including large

[15] Draft Policy Impact Report, paragraph III.2.4.2, page 14.

[16] BSA Comments on the Personal Data Protection Decree No. 13/2023/ND-CP, 30 June 2023 at https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-superseding-decree-no-722013nd-cp.

and small companies, and data subjects will need time to adjust to the change. We also strongly recommend that the Government consult with stakeholders throughout the transition period, to facilitate information-sharing about implementation issues as they arise.

Recommendation: We recommend including a two-year transition period from the time the PDP Law is enacted to the commencement of its effective date. This will allow time for any implementing regulations and guidance to be issued and allow organizations sufficient time to adjust their systems and processes to comply with the PDP Law.

A two-year transition period with the introduction of new personal data protection regulations is in line with practices in other jurisdictions. In Singapore, the Personal Data Protection Act was enacted in 2012, and came into force in 2014. In the European Union, the European Parliament adopted the GDPR in April 2016, and it took effect in May 2018. In Thailand, the Personal Data Protection Act was enacted in 2019 and took effect in 2022, providing a three-year transition period.

Conclusion and Further Resources

We would like to thank the MPS for considering our comments on the development of a PDP Law and hope that the MPS will positively consider our recommendations. Further to the recommendations above, BSA developed Global Privacy Best Practices[17], available in English and Vietnamese, which the MPS may wish to consider as a further resource. We have attached a copy within the Annex.

We urge the MPS to continue to engage in dialogue with the private sector and to continue open discussions to achieve common goals for developing a vibrant and competitive digital economy. This could include deeper collaboration between the MPS and other government agencies with the private sector such as through roundtable discussions on how the PDP Law should be developed. Please do not hesitate to contact us if you require any clarification or further information. Thank you once more for your time and consideration.

Sincerely,

Wong Wai San

Wong Wai San

Senior Manager, Policy – APAC

[17] BSA Global Privacy Best Practices, 2018, at https://www.bsa.org/policy-filings/2018-bsa-global-privacy-best-practices.

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.