



## PUBLIC CONSULTATION ON THE REVIEW OF PERSONAL DATA PROTECTION ACT 2010

### COMMENTS FROM BSA | THE SOFTWARE ALLIANCE

February 28, 2020

#### Introduction

BSA | The Software Alliance (**BSA**)<sup>1</sup> appreciates the opportunity to provide comments in response to Malaysia's Department for Data Protection (**JPDP**)'s Consultation Paper 01/2020 (**Consultation Paper**) on the Review of Personal Data Protection Act 2010 (**PDPA**).

BSA members are enterprise solutions providers that create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. These enterprise software companies are in the business of providing privacy-protective technology products and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their personal data.

BSA supports JPDP's PDPA review to promote robust personal data protection through a legal framework that is flexible, fosters innovation, and better enables international data transfers. We have developed a set of [Global Privacy Best Practices](#),<sup>2</sup> which we strongly suggest be taken into consideration as part of the JPDP's review of the PDPA. The BSA Global Privacy Best Practices can serve as useful guidelines to ensuring personal data protections are consistent with consumers' expectations, while also enabling companies to pursue legitimate business interests.

In addition to sharing the best practices mentioned above, we also welcome the opportunity to provide our comments on the following issues the consultation raises:

- A. Transfer of Data Outside Malaysia;
- B. Obligations of Data Controllers and Data Processors and Allocation of Liability;
- C. Processing Personal Data Using Cloud Computing;
- D. Avoiding Prescriptive Approaches to Data Portability;
- E. Disclosure of All Third Parties That Receive Data;
- F. Consent;
- G. Data Breach Notification;

---

<sup>1</sup> BSA | The Software Alliance ([www.bsa.org](http://www.bsa.org)) is the leading advocate for the global software industry before governments and in the international marketplace. Headquartered in Washington, DC, and with operations in more than 30 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, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.*

<sup>2</sup> BSA's Global Privacy Best Practices available at [https://www.bsa.org/files/policy-filings/2018\\_BSA\\_Global\\_Privacy\\_Best\\_Practices.pdf](https://www.bsa.org/files/policy-filings/2018_BSA_Global_Privacy_Best_Practices.pdf)

- H. Security of Data Collection Points; and
- I. Territorial Scope of the PDPA

## Comments

### A. Transfer of Data Outside Malaysia

BSA welcomes the Consultation Paper's recognition that the "no transfer of personal data outside Malaysia should occur unless approved" approach may be a barrier to data flows. The exclusive reliance on this "white list" mechanism to allow personal data to be transferred outside Malaysia is at odds with the agility necessary to allow countries and their populations to leverage the benefits of international data transfers.

The ability to transfer data internationally is the lifeblood of the modern digital economy. Organizations transferring personal data must take appropriate steps to ensure user's information will be properly protected.

The accountability model, first established by the OECD and subsequently endorsed and integrated in many legal systems and privacy principles, including Japan's Act on Protection of Personal Information and Canada's Personal Information Protection Act — both of which received an adequacy determination from the EU — provides an approach to cross-border personal data governance that effectively protects the privacy interests of individuals and fosters streamlined, robust data flows. An accountability model requires that organizations that collect and use personal data are responsible for its protection and responsible use no matter where or by whom it is processed. It also requires that organizations transferring personal data must take appropriate steps to be sure that any obligations — in law, guidance or commitments made in privacy policies — will be met.

Therefore, we support the JPDP's consideration of eliminating the "white list" approach to allowing international personal data transfers and encourage Malaysia to instead adopt additional legal grounds for such transfers aiming to make the system more flexible. For instance, the JPDP should recognize the validity of contractual or similar arrangements that would provide for the protections required under Malaysia's laws regardless of where the personal data is transferred to, stored, or processed. In addition, transfers based on commitments assumed in international cooperation agreements, including international industry codes of conduct or international frameworks developed through open, multi-stakeholder processes should also be permitted.

**BSA strongly encourages the JPDP to allow personal data to be transferred outside Malaysia based on flexible mechanisms that ensure personal data will be properly protected, while also enabling companies to provide innovative products and services that require agile transfer of data across borders.**

### B. Obligations of Data Controllers and Data Processors and Allocation of Liability

The Consultation Paper points out that the PDPA does not currently directly regulate data processors. It is important that the PDPA clearly defines data users (roughly equivalent to the concept of data controller in other laws) and data processors and that this definition considers the distinct roles each of these entities play, as those roles are directly linked to their ability to interact with data subjects and to comply with legal requirements. For clarity, we use the more commonly used term "**data controller**" when referring to the PDA's concept of "data user"

BSA agrees that data processors have important obligations to safeguard the privacy of personal data they process and maintain on behalf of other businesses (data controllers). Any comprehensive privacy legislation must recognize this essential role and responsibility, including by requiring data processors to act on behalf of controllers and at their direction.

Data controllers should have the primary obligation for ensuring compliance with applicable personal data protection laws, while data processors should be required to comply with data controller instructions and to ensure the security of the personal data they process. These are the customary

responsibilities placed upon data controllers and data processors in other data privacy and personal data laws globally and we encourage Malaysia to adopt these parameters.

It is paramount to recognize the distinct role of data processors and that of data controllers. Failing to do so would undermine consumer privacy, rather than protect it. That is because subjecting all companies to the same obligations, regardless of their role in handling consumer data, can create new risks to privacy and security — such as requiring companies to look at sensitive personal data they otherwise would not access, or even requiring a company to disclose information to a consumer they do not know. For that reason, privacy laws around the world — including the European Union's General Data Protection Regulation (**GDPR**),<sup>3</sup> the Singapore Personal Data Protection Act,<sup>4</sup> and the Philippines Data Privacy Act<sup>5</sup> — recognize the distinct role of companies that process personal data on behalf of other companies. Distinguishing between the data controller and data processor roles improves privacy protection of all consumers. It also provides clear direction for companies to understand their obligations in protecting consumers' personal data.

**BSA recommends the PDPA make a clear distinction between data controllers and data processors and determine that data controllers have the primary obligation for ensuring compliance with applicable personal data protection laws, while data processors are required to comply with data controller instructions and to ensure the security of the personal data they process.**

The Consultation Paper also invites stakeholders to comment on a potential obligation for data processors to register with the Personal Data Protection Commissioner (**PDP Commissioner**), and also to broaden the current registration scheme to require all data controllers to register with the PDP Commissioner (instead of only those data controllers that fall within the existing 13 classes designated by the PDP Commissioner). These proposals, if implemented, would only consume PDP resources and significantly increase the regulatory burden on the entire industry (including micro-, small-, and medium-sized enterprises) without increasing data protection.

**BSA, therefore, recommends that the JPDP not change the existing registration requirements. Conversely, the JPDP could consider adopting a business-friendly approach and do away with all registration requirements altogether.** This would also be in line with the personal data protection laws of other jurisdictions such as the EU GDPR and the Singapore Personal Data Protection Act, which do not impose a registration requirement on personal data controllers or personal data processors.

### **C. Processing Personal Data using Cloud Computing**

The Consultation Paper states that the PDP Commissioner is considering drafting and issuing guidelines on the use of cloud computing for data controllers. While guidelines promoting best practices may be a helpful tool, their implementation should be voluntary and developed in coordination with industry in a multi-stakeholder consultative process. The legal obligations and allocation of liability applicable to cloud computing should be the same applicable to data controllers and processors in general. The focus should be on the role played by the company collecting and/or processing personal data, and not on the technology used to do so.

**BSA recommends that the JPDP take a technology neutral approach and apply data protection rules based on whether an enterprise is acting as a data controller or a data processor rather than whether an enterprise is providing a cloud computing service or not.**

---

<sup>3</sup> At <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

<sup>4</sup> At <file:///C:/Users/JaredRagland/Downloads/Personal%20Data%20Protection%20Act%202012.pdf>

<sup>5</sup> At <https://www.privacy.gov.ph/wp-content/uploads/DPA-of-2012.pdf>

## D. Avoiding Prescriptive Approaches to Data Portability

According to the Consultation Paper, the JPDP is considering a new provision on data portability. BSA supports a clear and flexible regulatory environment to support data-driven innovation, which includes a right to access and port personal data.

The software industry has undergone a dramatic transformation. BSA members provide a wide array of Internet-enabled services, such as cloud computing services, data analytics, security solutions, and much more. This is in addition to a full range of software solutions that are more often downloaded online or used on remote servers. Today, software solution and cloud service providers already facilitate migration and portability in creative and innovative ways absent regulatory intervention. This is consistent with their commercial interests to attract customers from competitors — and there are many commercially available tools in the market to facilitate migration.

The specific mechanisms for transferring data from legacy systems to cloud-based service providers and from one service provider to another will depend heavily on the specifics of each organization and their existing data structures. BSA members offering software and cloud computing services have developed a variety of solutions that can be tailored to their customer for secure transfer of data from one system to another. In some cases, this may be straightforward. In others, it may be more difficult, such as when the data is tightly associated with particular applications and is not easily convertible to alternative systems.

As software, cloud computing, and other emerging technologies continue to evolve, it is likely additional voluntary internationally recognized standards and practices will emerge, and governments should support industry-led efforts to promote data portability. Therefore, a prescriptive regulatory approach is likely to be counter-productive and would likely limit the services available in the marketplace without improving data migration capabilities.

**BSA recommends that rather than prescribing data portability rules, the JPDP should consider taking a more flexible approach and, instead, encourage the adoption of voluntary, transparently developed, industry-led international standards and practices to facilitate data portability.**

## E. Disclosure of All Third Parties that Receive Data

Currently, the PDPA requires data controllers to include in a notice or privacy statement the class of third parties to whom the data controller discloses or may disclose data subjects' personal data. This requirement is aligned with other legal systems, including the GDPR. The PDP Commissioner is considering expanding this obligation to require data controllers to identify all third parties to whom personal data may be disclosed.

While BSA supports the transparency that this proposal seeks to promote, the new requirement would not substantially enhance data subjects' rights but it would place a large burden on companies — particularly small enterprises — as they would need to identify every processor and sub-processor they utilize.

Providing information on the *categories* of third parties to whom data is supplied meets the transparency goal sought by the Government of Malaysia in a less burdensome manner.

**BSA recommends that the JPDP maintain the current PDPA requirement to provide notice of the classes of third parties to whom the data controller discloses or may disclose data subjects' personal data and refrain from imposing the stricter proposed requirement to identify all third parties to whom such data is disclosed.**

## F. Consent

The Consultation Paper proposes to modify the PDPA to clarify consent requirements.

While we recognize that the data subject's consent can be a valid legal basis for processing (including acquiring, storing, and transferring) personal data, consent should not be the sole or primary legal basis. Other grounds for collecting and processing personal data should be considered equally valid.

As consent may be difficult to offer and/or provide, depending on the circumstances, organizations should be allowed to process personal data unless a data subject objects — particularly if the processing is part of the organization's legitimate interest or there is another lawful basis for processing — as long as they have tools, policies, and programs in place that ensure they are making responsible decisions, in line with a data subjects' reasonable expectations, about personal data protection and use.

In circumstances where consent may be necessary, it is important that the legislation focuses on the objective, not the means, of obtaining such consent. In this case, the PDPA should recognize the validity of a range of mechanisms for data subjects to provide consent, including an informed and easily accessible opt-out option, and implied consent.

Requiring excessive express consent can lead to "click fatigue" with users simply accepting whatever terms are presented to them in order to get to the service they are seeking. Indeed, there are a wide range of mechanisms that enable users to control and consent to the collection and use of their personal data, and some of the more robust opt-out mechanisms provide stronger protection for consumer privacy (with fewer disruptions for Internet users) than weaker opt-in/express consent mechanisms.

The PDPA should also expressly recognize that consent may be implied when personal data is collected and processed in a manner that is consistent with a consumer's reasonable expectations. For instance, an individual using an electronic fare card to access public transportation services should not need to provide express consent each time the individual uses the card. Implying consent to such processing helps consumers by reducing the number of times that they are asked to consent to processing they already expect. If consumers were constantly asked to consent to such processing, it would make consent requests less meaningful. By instead focusing express consent requirements on processing of certain sensitive data, or processing for certain unexpected uses, the PDPA would help ensure that consent requirements provide meaningful choice to consumers.

Finally, we note that for the situations in which consent may be required, it should only be required a second time for subsequent personal data uses if material changes take place after the personal data is initially collected.

**BSA recommends that the JPDP amend the PDPA to include flexible grounds for collecting and processing personal data and, in cases where consent is required, the JPDP should refrain from mandating that it be obtained multiple times for subsequent uses of personal data unless material changes occur.**

## G. Data Breach Notification

The Consultation Paper notes that there is currently no mandatory requirement for data controllers to report personal data breaches to the JPDP. In lieu of the mandate, the JPDP has issued a form the data controllers are encouraged to use to voluntarily report personal data breaches. Furthermore, the JPDP is considering making such notification mandatory by revising the relevant provisions of the PDPA.

The adoption of a mandatory framework for data breach notification can promote trust in the digital economy by establishing expectations for data stewardship that will reduce the risk of future breaches and ensure that data subjects receive timely and meaningful information about whether their personal information has been compromised. We favor the introduction of breach notification systems when they incentivize data controllers to maintain robust protections for personal data, while enabling data

subjects to take action to protect themselves when their data is compromised. Any such system should be carefully crafted to incentivize data controllers to notify, while ensuring that data subjects receive timely and meaningful notifications about actual data breaches that create material risks of identity theft or financial fraud. To achieve these objectives, we support a breach notification system that is consistent with the following key principles:

- The notification standard should be risk-based so that data controllers can take steps to mitigate the potential impact of data breaches that create significant risks of material harm. The standard should promote good data storage practices by clarifying that data rendered indecipherable to unauthorized entities through use of encryption or other obfuscation technologies does not create such risks.
- In the immediate aftermath of a data breach, data controllers should be encouraged (and afforded adequate time) to focus their resources on performing a thorough investigation and restoring the integrity of potentially compromised systems.
- In the event of a breach, data subjects should expect to receive notification from the data controller with which they have a direct relationship. Such a principle ensures that data subjects understand the significance of notifications they receive and promotes good data stewardship by ensuring that data controllers who collect personal data take a life cycle approach to managing the associated privacy and security risks.

For a more detailed explanation of these recommendations, please see the BSA – US-ASEAN Business Council joint submission to the JPDP dated September 7, 2018.<sup>6</sup>

## H. Addressing Privacy Issues Arising from Data Collection Endpoints

While BSA strongly agrees with the JPDP that encryption is a powerful tool to protect personal data, its use should be encouraged but not mandated in all instances. Security protections should be tailored to the sensitivity of the personal data being collected and its potential risk profile. Encryption should not be the only information security method considered adequate to effectively protect personal data.

Even where companies use encryption to protect personal data they collect, process, or store, it should be recognized they are seeking to protect a wide spectrum of targets against a wide variety of potential threats. Different encryption methods are appropriate in different scenarios, and encryption methods are always evolving and improving. Mandating specific encryption methods to be used in all cases would therefore be inefficient and actually harm security. Policies targeted at increasing information security should enable the implementation of security measures that are most appropriate to mitigating the specific risks each company faces to increase effectiveness. Technology neutrality is important to ensure this objective is achieved.

**BSA recommends the JPDP encourage the voluntary use of encryption and other technologies to secure personal data and refrain from imposing prescriptive mandates, thus allowing companies to tailor measures they use to the sensitivity of the personal data being collected and its potential risk profile.**

## I. Territorial Scope of the PDPA

As expressly recognized by the JPDP, the current PDPA does not apply to the processing of personal data where it is processed outside Malaysia unless it is intended to be further processed in Malaysia. We commend the current approach as it recognizes that personal data protection laws should be limited to activities that have a sufficiently close connection with the respective countries that enact them.

---

<sup>6</sup> BSA – US-ASEAN Business Council joint submission to the JPDP – September 7, 2018 at [https://www.bsa.org/files/policy-filings/09072018BSA\\_USABCSubmission\\_JPDP\\_DBNConsult.pdf](https://www.bsa.org/files/policy-filings/09072018BSA_USABCSubmission_JPDP_DBNConsult.pdf).

Many BSA member companies conduct business internationally and are subject to a complex global regulatory landscape for personal data protection. While companies will need to ensure they comply with the PDPA, the current approach under the PDPA provides companies with clarity on when the PDPA will apply or not apply where information is processed outside of Malaysia.

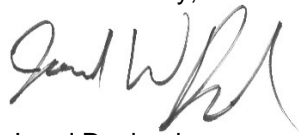
**BSA recommends the JPDP continue with the current approach in the PDPA to territorial scope, and not seek to apply it to personal data that is processed outside Malaysia unless it is intended to be further processed in Malaysia.**

## Conclusion

BSA once again expresses our support of the JPDP's efforts to review and update the PDPA, responding to the ever-evolving needs of the digital economy and data innovation. We hope that our comments will support these efforts.

Please do not hesitate to contact us if you have any questions or comments regarding our suggestions. We remain open to further discussion and look forward to further opportunities to work with the JPDP on the development of data protection and data policy issues in Malaysia.

Yours sincerely,



Jared Ragland  
Senior Director, Policy — APAC  
BSA | The Software Alliance

**Attachment: BSA Global Privacy Best Practices**

## **Attachment**

### **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
<b>Territorial Scope</b>	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.
<b>Definition of Personal Data</b>	<p>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 a 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.</p> <p>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.</p>

ISSUE	BEST PRACTICE
<b>Harm</b>	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.
<b>Transparency</b>	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.
<b>Purpose Specification</b>	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.
<b>Data Quality</b>	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.
<b>Grounds for Processing</b>	<p>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.</p> <p>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.</p>
<b>Consent</b>	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.
<b>Processing Sensitive Personal Data</b>	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
<p><b>Consumer Control</b></p>	<p>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.</p> <p>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.</p> <p>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.</p>
<p><b>Security and Breach Notification</b></p>	<p>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.</p> <p>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.</p>
<p><b>Accountability Requirements</b></p>	<p>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.</p> <p>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.</p>

ISSUE	BEST PRACTICE
<b>Cross-Border Data Transfers</b>	<p>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.</p>
<b>Obligations of Controllers and Processors/ Allocation of Liability</b>	<p>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.</p>
<b>Remedies and Penalties</b>	<p>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.</p>