BSA Submission On
The Digital Information Security in Healthcare Bill
For the Ministry of Health & Family Welfare

April 20, 2018

Shri. S.C. Rajeev,
Director (eHealth)
Room No. 211-D,
Ministry of Health & Family Welfare
A Wing, Nirman Bhawan, Maulana Azad Road,
New Delhi – 110108

E-mail: egov-mohfw@nic.in

Dear Sir,

BSA | The Software Alliance ("**BSA**")[1] welcomes this opportunity to comment on the Draft Digital Information Security in Healthcare Bill ("**DISHA Bill**") that was issued for public consultation by the Ministry of Health & Family Welfare ("**MoHFW**") on Wednesday, March 21, 2018.

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, and they have a deep and long-standing commitment to protect the privacy of personal information.

As a global organization, we actively follow privacy and data protection developments around the world. We have consistently highlighted that an effective privacy regime provides appropriate protections for individuals' personal data while also spurring innovation that is fueling the global economy.

BSA has reinforced this view in its past contributions made to the Government of India in an effort to advance a strong privacy and data protection regime for India's digital ecosystem. For your kind reference, we wish to direct your attention to the following:

1. **BSA Personal Data Protection Principles:** Our Personal Data Protection Principles seek to guide policymakers around the world towards developing effective regimes for privacy and data protection. The Principles rest on five pillars of 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; and (5) Personal Data Breach Notifications. A copy of these Principles is attached herewith.

[1] BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

Le – Meridien
15th floor, Room 1529
Windsor Place Janpath,
New Delhi 110001
India

P : 011-497-890-66
W: bsa.org

2. **BSA Submission to the White Paper of the Committee of Experts on a Data Protection Framework for India:** In July 2017, the Government of India constituted a Committee of Experts to deliberate on a data protection framework for India under the Chairmanship of Justice B.N. Srikrishna ("**Expert Committee**"). The Expert Committee had released a White Paper in November 2017, seeking detailed inputs from the public on the protection of data in India. BSA contributed to this process, responding to a number of specific issues raised by the White Paper. A copy of BSA's submission to the Committee of Experts on Data Protection is attached herewith.

We share the MoHFW's view that protecting the privacy and security of electronic health data is of utmost importance to India's digital ecosystem, as outlined in the objectives of the DISHA Bill.[2]

However, there is a need for a consistent and coordinated approach in the formulation of various data protection frameworks. To achieve the objectives outlined in the DISHA Bill, MoHFW should coordinate with other agencies involved in developing frameworks pertaining to data protection, especially the Expert Committee on Data Protection constituted by the Government of India last year.

We have elaborated on the need for a consistent and coordinated approach below:

(a) **There is a need for conceptual consistency across data protection frameworks in India to promote privacy and security:**

The DISHA Bill proposes many concepts pertaining to data protection, such as the types of personally identifiable information, data ownership, consent frameworks, anonymization, security standards, responsibilities of parties, and rights of individuals.

These concepts are fundamental to both privacy protection and the data-driven businesses of today, including those of our member companies. Based on our experience working in different jurisdictions, we recommend these core concepts relating to data protection be consistent across sectoral laws and policies at the Central and State level in order to promote privacy and security. It is also important to ensure that data protection regimes are risk-based, recognizing that some data is more sensitive than others, and that this sensitivity is highly context dependent.

For example, inconsistent definitions for 'anonymization' across laws would create challenges for entities that handle a variety of data types. Conversely, individuals, businesses, and authorities will have a clearer understanding of their rights and obligations in relation to different categories of data if there is conceptual consistency across data protection frameworks.

Moreover, any legal, technical, or administrative frameworks that are specifically relevant to the health sector must be harmonized with other laws and regulations pertaining to data protection to promote data privacy and security across the entire digital ecosystem.

We understand that the Expert Committee is currently working on developing such a framework, by enumerating specific Data Protection Principles, which would provide conceptual consistency across data protection frameworks in India. We urge the MoHFW to evaluate these principles specifically in the context of the DISHA Bill.

(b) **Consistent obligations across data protection frameworks would promote compliance and help protect individual data privacy:**

The data-driven businesses of today have established systems and processes designed to protect the privacy and security of personal information. Some of these businesses, including BSA member companies, operate simultaneously in different sectors and industries. Generally,

[2] As per Notice F.No. Z-18015/23/2017-eGov issued by the Ministry of Health & Family Welfare, available at: https://mohfw.gov.in/sites/default/files/R_4179_1521627488625_0.pdf

Le – Meridien
15th floor, Room 1529
Windsor Place Janpath,
New Delhi 110001
India

P : 011-497-890-66
W: bsa.org

the underlying technical architecture designed to ensure data privacy and security is the same or implemented using the same or connected computing infrastructure.

We understand that the DISHA Bill empowers the National Electronic Health Authority of India to formulate 'standards, operational guidelines and protocols for the generation, collection, storage, and transmission of digital health data. The DISHA Bill also contemplates other compliance obligations, for example with respect to personal data breaches.

BSA advocates that to promote individual data privacy and security such compliance obligations should be risk-based and consistent across sectoral laws and policies at the Central and State level. Consistent obligations would enable service providers to leverage efficiencies of scale and protect individual data privacy. On the other hand, imposing inconsistent or incompatible compliance obligations on service providers would restrict their ability to establish and implement best-in-class technical architecture, which are designed to protect the privacy and security of personal information on a system-wide level.

(c) **To promote data privacy and security across the entire digital ecosystem, there is a need for a collaborative policy discussion involving all relevant stakeholders:**

The DISHA Bill seeks to regulate a variety of service providers, such as 'clinical establishments', 'health information exchanges', and other entities that handle 'digital health data'.

Given the interconnectedness of information assets and network technologies today, it is important to consider the impact of the DISHA Bill on other stakeholders that constitute India's digital ecosystem such as cloud service providers that enable the collection, storage, and transmission of digital health data.

While BSA recognizes the need for regulators to develop regulations that apply to their specific sectors, we believe that a collaborative policy discussion involving all relevant stakeholders is required to achieve the objectives set out in the DISHA Bill. To that extent, we urge the MoHFW to interact with other sectoral regulators, as well the Expert Committee to understand the implications of the DISHA Bill for the larger digital ecosystem in India.

Recommendation:

BSA recommends that the Government of India coordinate the various policy processes involving data protection across sectors.

Specifically, we urge the MoHFW to interact with other sectoral regulators and the Expert Committee to understand the implications of the DISHA Bill for the larger digital ecosystem in India.

This will ensure the development of a comprehensive data protection framework for India to act as the base foundation, upon which sector-specific initiatives can be built.

Accordingly, it might be prudent for the MoHFW to defer further development and discourse on DISHA till the outcome of the Expert Committee is available.

Conclusion

BSA thanks the MoHFW for this opportunity to offer comments on India's proposed framework for protecting electronic health data. Our member companies have a long-standing commitment to India, and are excited by the potential that India's evolving digital ecosystem offers.

Le – Meridien
15th floor, Room 1529
Windsor Place Janpath,
New Delhi 110001
India

P : 011-497-890-66
W: bsa.org

We stand ready to answer any questions regarding this submission, or to provide any further assistance on our Personal Data Protection Principles and our submission to the Expert Committee, as may be required.

Thanking you.

Yours sincerely,

Venkatesh Krishnamoorthy
Country Manager- India
BSA | The Software Alliance

Le – Meridien
15th floor, Room 1529
Windsor Place Janpath,
New Delhi 110001
India

P : 011-497-890-66
W: bsa.org

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 OECD[1] 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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.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

January 29, 2018

Shri Rakesh Maheshwari
Scientist G & Group Coordinator, Cyber Laws
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi - 110003

Dear Sir,

Subject: BSA Responses to the White Paper of the Committee of Experts on a Data Protection Framework for India

This is with reference to the White Paper of the Committee of Experts. Please find enclosed the following:

- Responses of BSA | The Software Alliance ("BSA") to the White Paper [Annexure I]
- BSA Personal Data Protection Principles [Annexure II]

We have uploaded our responses on the website: https://innovate.mygov.in/data-protection-in-india/ on **Monday, January 29, 2018.** We look forward to participating in this important discussion and stand ready to answer any questions you may have.

Thanking you,

Yours sincerely

Venkatesh Krishnamoorthy
Country Manager – India
BSA | The Software Alliance

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

ANNEXURE I

RESPONSES OF BSA | THE SOFTWARE ALLIANCE TO THE WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA

JANUARY 29, 2018

BSA | The Software Alliance is the leading advocate for the global software industry.[1] Our member companies are at the forefront of data-driven innovation, and they have a deep and longstanding commitment to protecting the privacy of personal information. BSA appreciates the opportunity to provide comments on the White Paper of the Committee of Experts on a Data Protection Framework for India ("White Paper"). As a global organization, BSA actively follows privacy developments around the world. We have consistently highlighted that an effective privacy regime provides appropriate protections for individuals' personal data while also spurring innovation that is fueling the global economy.

Our comments below reinforce this view and respond to a number of specific issues raised in the White Paper. Among other things, the comments emphasize the following key points:

- The definition of personal data should apply to information that is reasonably linked to an identified or identifiable individual;
- A risk-based approach should be used to determine whether heightened protections should apply to sensitive data based on the context in which data is used;
- The law should differentiate between and clearly define data controllers and processors;
- The law should provide appropriate, flexible bases for processing data;
- The law should adopt a flexible approach to notice and consent;
- The law should facilitate cross-border data flows and avoid burdensome restrictions on data transfers, such as data localisation requirements;
- The framework should embrace the principle of accountability; and
- Personal data breach notification requirements should apply where there is a material risk of harm to individuals.

[1] 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.

As the Government of India seeks to develop a data protection framework, we urge consideration of the issues discussed below to ensure that individuals benefit from important privacy protections, and that India reaps the substantial benefits of the power of the digital economy.

PART II: SCOPE AND EXEMPTIONS

Chapter 1 – Territorial and Personal Scope
(Questions 1-4)

BSA recommends limiting the scope of India's data protection law or framework to entities or activities that have a sufficiently close connection to India. Specifically, BSA recommends that the Government limit application of the data protection law to data processing performed by an individual or legal entity, whether public or private, provided that: (1) Indian residents are specifically targeted; (2) the personal data that is the object of the processing is purposefully collected from data subjects in India at the time of the collection, and (3) such collection is performed by an entity established in India through a stable arrangement giving rise to a real and effective level of activity, or subject to India law by virtue of international public law. Under this standard, the mere accessibility of a website in India or the use of a language used in India would be insufficient, on their own, to establish the applicability of India's prospective data protection law.

In addition, BSA believes that the criteria suggested above to govern the applicability of India's data protection law will ensure effective enforcement of orders against foreign entities.

Chapter 2 - Other Issues of Scope
(Questions 1-5)

Consistent with data protection laws in many other jurisdictions, BSA recommends that the protections in India's data protection law apply only to natural persons. This limitation would tie India's data protection law to the rights and interests of individuals, which are the ultimate source and justification for the data protection principles upon which the White Paper builds. As the White Paper highlights, the right to privacy that the Supreme Court of India recognized in *Puttaswamy vs. Union of India* is derived from the right to life and personal liberty guaranteed under Article 21 of the Constitution of India, as well as the Constitutional guarantees of autonomy and dignity of an individual. In other words, data protection principles protect interests that are tied to personhood; it is not clear that they extend coherently to juristic persons. Further, extending data protection law to juristic persons is not necessary to protect their interests in information and would create significant uncertainty about how to apply the law. This uncertainty could chill data-driven innovation and harm economic growth. Accordingly, consistent with the Expert Committee's provisional view, the law's scope should be limited to natural persons.

In addition, it is critical for the Government to make any new data protection law purely prospective and to provide a reasonable period of time between the enactment of a data protection law and its effective date. Individuals, businesses, and the Government will benefit more from an orderly transition than with one that is abrupt and requires catch-up under threat of enforcement. Although BSA does not,

at this time, suggest a specific transition period, we note that, in other settings, legislators have allowed a two-year transition period. Below, we offer several factors to consider in connection with determining the appropriate transition period.

Many BSA member companies conduct business internationally, and any data protection law that India enacts will become part of a complex global regulatory landscape. Companies will need to continue to comply with their existing obligations under the data protection laws of other countries and regions. To make their compliance efficient and provide the best experience for consumers and customers, businesses will likely strive to implement one set of data practices across all of their operations, including those covered by India's law. Undertaking compliance in this environment is a complex endeavor.

Of course, companies will also need to ensure that they comply with any new or unique requirements that India's law creates. Companies may need to invest considerable time and resources in modifying their data systems and practices. Along the same lines, companies currently use several different mechanisms to transfer data around the world – e.g., binding corporate rules, contractual clauses, APEC Cross-Border Privacy Rules (CBPR)– and they will need sufficient time to update any contracts or arrangements to take into account any new obligations.

Finally, the global data protection landscape may become more complicated while India develops its law. For example, the European Union's General Data Protection Regulation (GDPR) will go into effect on 25 May 2018, and the EU is currently considering a further change to its data protection requirements through the proposed ePrivacy Regulation. These developments will add to the complexity of businesses' compliance obligations and should be taken into account in determining the appropriate transition period. Moreover, it may be helpful for the Government to assess the effectiveness of the GDPR's implementation to determine whether any lessons learned could be useful guidance as India develops and implements its own data protection framework.

Chapter 3 - Definition of Personal Data

(Questions 1-6)

BSA recommends referring in the law to "personal data," as this term has been adopted in several other data protection laws and frameworks, such as the GDPR and the Organisation of Economic Cooperation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

More important than the label is the scope of data that the law covers. As indicated in our response to Part II, Chapter 2, the law should apply only to natural persons. Beyond that, the law should protect information that, if mishandled, would have a meaningful impact on an individual's privacy. Accordingly, the law's definition of "personal data" should be limited to data that is reasonably linked to an identified or identifiable individual.

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 specific individuals, the law is likely to have a chilling effect on everything from cybersecurity to improved customer services without having an actual benefit on personal privacy.

BSA also recommends excluding anonymized data from coverage of the data protection law. A suggested definition of anonymised data is “data that is not reasonably linkable to a specific individual.” By definition, such data is not personal and therefore does not implicate individual privacy interests.

Clearly excluding anonymised data from the definition of “personal data” – and the data protection law as a whole – would benefit individuals and the economy. The exclusion would give businesses the incentive to develop and use anonymisation techniques, thereby reducing privacy and security risks. At the same time, the ability to use anonymised data outside the framework of a data protection law will encourage innovative uses of data.

Finally, we note that, within the scope of information covered under the definition of personal data, the law should distinguish between fully identified personal data and pseudonymous data, relaxing appropriate requirements when data is processed in pseudonymized form. Pseudonymous data is organized according to a randomly generated identifier that is not used in any other dataset and from which other information that could be used to connect information to a specific individual has been removed. Because such techniques mitigate the risk that third parties will link the information to a specific individual, pseudonymised data should be subject to less stringent rules than personal data in which specific individuals may be readily identified. This graduated approach is preferable to a binary distinction between personal data and fully anonymised data, and it will address the risk of harm where it is most significant while also incentivizing companies to take additional steps to protect individuals’ personal information.

Chapter 4 - Definition of Sensitive Personal Data

(Questions 1-2)

BSA recognizes that cultural considerations may counsel in favor of creating certain sensitive data categories, but we also recommend that the Government take a rigorous, risk-based approach to its determinations. Defining certain types of personal data to be “sensitive” may be consistent with a risk-based approach, but care must be taken to limit such categorization. Other data protection laws have limited that categorization to racial or ethnic origin, political opinions, religious beliefs, genetic or biometric data, health information, or information regarding sexual orientation. Even if these categories of information are designated as sensitive, BSA recommends that the Government avoid imposing restrictions solely based on these categories. Rather, BSA recommends a risk-based approach to determine whether heightened protections should apply in these limited circumstances based on the context in which data is used.

Fundamental to the risk-based approach is the identification of potential harms to individuals. BSA suggests that specific, concrete, measurable harms provide an appropriate foundation for establishing sensitive data categories. Such harms are not only objective but also tend to be widely perceived by individuals as harmful.

In *Puttuswamy,* the Supreme Court of India also appears to recognize the importance of a risk-based approach in defining the right to privacy. In pages 201-203, the judgment describes various aspects of privacy by identifying four zones (i.e.

from ‘personal’ to ‘public’) and the potential risk to two aspects of freedom, i.e., the freedom to be left alone, and the freedom for self-development.

BSA also recommends distinguishing between sensitive data *categories* and sensitive or high-risk *uses* of data. Modern devices and services generate a significant volume and variety of personal data, but little of this data, on its own, presents a risk of concrete, specific, measurable harm to individuals.

Examining risks arising from the *use* of data, by contrast, would direct companies to focus their efforts on reducing risks in the context of their own data processing operations. This focus will lead to greater flexibility in data processing and promote innovative uses of data while also providing appropriate data protections.

Accordingly, BSA recommends keeping the data protection framework focused on risk, including with respect to sensitive data, and applying protections to situations where there is a risk of concrete, specific, and measurable harm to individuals.

Chapter 5 - Definition of Processing

(Questions 1-3)

BSA’s overarching view is that India’s data protection framework should be flexible and risk-based. Personal data processing typically depends on a set of distinct but interrelated operations. For example, the ability to *use* personal data may require transmittal, storage, and retrieval. In practice, companies rarely design data protection programs that focus on atomic operations in data processing. Instead, BSA members and most modern enterprises take a holistic approach toward risk management and compliance with applicable data protection laws. Covering all facets of data processing need not be inconsistent with this goal and may, in fact, reduce the risk that the law will unintentionally exclude or establish differential treatment for certain actors.

A definition of “processing” that includes a comprehensive set of operations would be consistent with the definition in the GDPR, among other data protection frameworks. As the White Paper points out (p. 45), distinctions between operations such as collection, use, and disclosure are “often thin.” Moreover, personal data use often requires other operations, such as storage and retrieval. Making it clear that the law is intended to cover such operations will provide more certainty to businesses than a law that does not reflect the complexity of modern data use. Other basic elements of data protection law, such as the definition of “personal data,” provide better means of ensuring that the scope of the law is appropriate to promote innovation and protect individual privacy.

In addition, the law should apply to automated processing, as well as manual processing that is performed on data that is kept in a system that is structured in a manner to permit access according to specific criteria, which is consistent with the scope of other data protection laws.

Chapter 6 - Definition of Data Controller and Processor
(Questions 1-3)

BSA is broadly in favor of an accountability principle. We strongly support robust data protection and believe data controllers must be held responsible for the privacy and security of data entrusted to them. We are also strongly in favor of any measure that would reduce administrative burdens on data controllers. We note, however, that an accountability obligation should be accompanied by guidance about how to implement the principle and how compliance will be assessed.

The law should differentiate between and clearly define “data controller” and “data processor.” Differentiating between data controllers and data processors serves to establish a clear allocation of roles and responsibilities and helps to clarify complex cases, where the data is processed by more than one entity (*e.g.*, outsourcing of processing).

BSA suggests the following definitions:

- "Data controller" means a natural person, juristic person, public authority, agency or other body which, alone or jointly with others, determines the purposes for which and the manner in which any personal data are, or are to be, processed

- “Personal data processor” means a natural person, juristic person, public authority, agency, or any other body which processes personal data on behalf of the data controller

The primary obligation for ensuring compliance with the applicable personal data protection law should fall on the data controller. The data controller retains a direct relationship with the data subject, determines what information to collect and for what purposes, decides how it is used, with whom it is shared and under what terms. By contrast, the data processor acts on behalf of the data controller and does not make the essential decisions affecting compliance with core data protection obligations. Accordingly, a data processor’s main obligation should be to follow the instructions of the controller and ensure the security of the personal data it processes.

Contracts between data processors and data controllers are the most effective means for governing processor responsibilities with respect to personal data. Importantly, controllers and processors should have the flexibility to negotiate their own contractual terms, without mandatory, prescriptive language provided by the law.

The clear allocation of liability among controllers and processors is critical and prevents confusion from arising in the complex system of relationships that underlie modern data processing operations. Maintaining this allocation would also avoid disturbing the existing economic and contractual relationships between processors and controllers. Finally, making data controllers primarily responsible for ensuring compliance with data protection law comports with common sense, because legal authorities and individuals know to whom to turn to in case of a problem.

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, imposing such liability on processors could also have a negative impact 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, while data processors should only be required through contractual mechanisms to comply with data controller instructions, assist the controllers in meeting their own compliance obligations, for example, by providing controllers with the means to comply with data subject rights with respect to the data processors handle, and to ensure the security of the data they process.

Chapter 7 – Exemptions

Research/Historical/Statistical Purpose Exemption
(Questions 1, 3)

BSA supports including an exemption for data processing that is conducted for research, historical, or statistical purposes. Personal data can provide extremely valuable insights into a broad range of social and economic issues, aiding research and supporting advances that enable improvements in health, education, transportation, and other areas. The law should provide that data must be kept secure against unauthorized use or disclosure during research, historical, or statistical processing, but data protection law should not otherwise hinder use of the exemption. BSA can identify no reason to restrict or prohibit the use of a research/historical/statistical exemption when research is subsequently published or used for a commercial purpose. The exemption should focus on whether further processing of personal data will serve a bona fide research, historical, or statistical purpose at the time that the processing is to be conducted and on the merits of the proposed use.

Restricting or prohibiting the use of the exemption based on later-published research or commercial activity would deprive society of the knowledge or other benefits that stem from the additional processing. For example, if a medical researcher conducts an epidemiological study using a large collection of medical records, it would make little sense to prohibit her from publishing her scientific findings. To the contrary, publishing this research advances the public interest in allowing data processing or research purposes in the first place.

Criminal Investigations and National Security
(Questions 1-8)

BSA supports the ability of law enforcement organizations to access digital evidence in connection with lawful criminal investigations, provided there is sufficient privacy protection. It is therefore appropriate that exemptions to data protection law enable law enforcement investigators to access data under specific and controlled circumstances, as outlined below. With regard to potential exemptions for national security or public safety, legitimate threats to national security or public safety will constitute activity covered under criminal law, and investigations seeking access to data for such purposes would therefore likely be able to do so through an appropriately scoped exemption for criminal investigations. Accordingly, BSA

recommends developing a law enforcement/national security exemption that focuses on criminal investigations.

To enable law enforcement organizations to access digital evidence in connection with lawful criminal investigations, BSA supports an exemption to data protection regulations that:

(1) applies only to lawfully authorized investigations of criminal or suspected criminal violations;

(2) distinguishes between content and non-content data;

(3) requires prior judicial approval for access to content data; and

(4) does not seek to mandate exceptional technical access to protected data (such as encrypted data).

An exemption should distinguish between content and non-content data, drawing on bodies of international case law. In general, the law should define content data to include substance or subject-matter associated with internet communications, including message text, content of attachments, message subjects, and related content, such as emails, text messages, or social media posts, as well as geolocation information. Non-content information may be defined to include information about recipients, senders, dates sent or posted, dates received, dates read, and dates deleted of internet communications such as emails, text messages, or social media posts.

A formal process should be required for law enforcement organizations to access both non-content and content data, but more robust protections should be in place for content data. In general, law enforcement access to content data should be permissible only with prior judicial approval in the form of a search warrant or equivalent court order. The probable cause standard adopted by the United States is the appropriate standard for issuance of such warrants. Less stringent requirements may be appropriate for non-content data, but some formal process to ensure the propriety and validity of the request, including the organization submitting the request, is essential. Procedures enabling the voluntary disclosure of personal data in exigent circumstances, as provided by the United States' *Electronic Communications Privacy Act*, may also be advisable. In every case, persons impacted by law enforcement access to personal data should have access to judicial review or judicial oversight mechanisms.

Law enforcement organizations should be able to access data held outside the country's sovereign territory only through established bilateral and multilateral mechanisms governing such access, such as Mutual Legal Assistance Treaties (MLATs) that establish safeguards for the transfer and processing of personal data to ensure privacy protections.

Upon receipt of personal data, law enforcement organizations should be bound to protect such data against inappropriate use or disclosure. Law enforcement organizations should be required to ensure that acquired personal data is only used for legitimate law enforcement purposes (prevention, investigation, detection or prosecution of criminal offenses), is stored in a manner that protects

such data from unauthorized or inappropriate access, is disseminated only to individuals or entities with a legitimate law enforcement purpose for using such data, and is erased or destroyed when no longer needed for legitimate law enforcement use.

Under a potential law enforcement exemption, individuals should have the right to access data that has been collected about them, to know the purposes for which such data has been collected, and to know by whom it has been collected. Except under exceptional circumstances, private entities holding personal data should have the right to inform customers when they have been directed to provide personal data about the customers to law enforcement organizations.

Chapter 8 – Cross Border Flow of Data
(Questions 1-3)

The Impact of Global Data Flows

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 global economic growth. According to the McKinsey Global Institute, global data flows were 45 times larger in 2014 than they were almost a decade earlier. In 1990, the total value of global flows of goods, services, and finance amounted to $5 trillion, or 24% of the world's GDP. In 2014, the value increased to $30 trillion, which was equivalent to 39% of GDP. As the White Paper acknowledges, "the ability to move data rapidly and globally has been a key building block of the global economic order." (White Paper at 70.)

The need to transfer data across borders arises in a variety of contexts. Global data flows enable multinational companies to scale global operations, startups to use cloud services to obtain digital infrastructure at lower costs, and small and medium-sized enterprises to use digital platforms to find customers and suppliers abroad. As one example, Lazada, Southeast Asia's most popular online shopping platform, operates local-language online retail stores in Indonesia, Malaysia, Philippines, Singapore, Thailand, and Vietnam. Lazada used cloud-based services to rapidly expand its product range by streamlining the vendor registration process, reducing the sign-up and onboarding time from two months to ten days.

In another example, multinational companies use cloud-based human resource management software to hire, support, and conduct performance management for a workforce of tens of thousands of people, who are often spread across numerous subsidiaries and affiliates around the world. Cloud-based solutions, such as those BSA members provide, increase HR functionality by providing real-time access to employee data worldwide, giving managers broad business insight across borders and business processes. By employing data analytics to give managers and HR departments more insight into their workforces, and enabling easy documentation and auditing of HR transactions, cloud-based HR systems that can access data globally increase efficiency and ease of use while reducing costs. They also improve security, as providers use their expertise to protect against cyberattacks and implement state of the art measures across the entire system through a unified approach to security.

Indeed, cross-border data flows are particularly important in the area of cybersecurity. Distributing data storage, such as with global cloud computing, compartmentalizes data sets, ensuring that a breach in one location is contained and does not give access to the entire data set. In addition, access to real-time global data enables companies to detect and address critical threats. For example, one leading cybersecurity company with operations in more than 50 countries searches for matches in its global database of emerging threats, often blocking the spread of a new attack.

Notably, data analytics, relying on cross-border data flows, have also contributed significantly to the social good, including enhancing public health and safety. For example, researchers around the world leverage data analytics to respond to natural disasters, including in the wake of the 2015 earthquake in Nepal, where they conducted a real-time analysis of mobile phone patterns to assist in disaster relief efforts.

In short, the economic and societal impact of cross-border data flows is substantial, and any proposal for a data protection framework should aim to preserve the ability to transfer data globally.

Developing a Flexible Data Protection Framework That Facilitates Cross-Border Data Flows

To protect individual privacy while "harness[ing] the benefits of the digital economy," (White Paper at 4), BSA recommends that the law explicitly recognize the ability to transfer personal data outside of India. However, the law should also recognize that no single data transfer mechanism alone is likely to meet the needs of modern technologies and services. While a data protection law may helpfully recognize certain data transfer mechanisms, it should also allow companies to adopt alternative, legally binding protections.

Accountability should provide the touchstone for data transfers. The accountability model, first established by the OECD and subsequently endorsed and integrated in a variety of data protection frameworks around the world, provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data flows. Canada, for example, has implemented this principle effectively into its national data protection law, avoiding preemptive restrictions on data transfers while at the same time ensuring that organizations remain responsible for personal information in their possession or custody that is subsequently transferred to third parties for processing.

Indeed, 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. For example, the APEC CBPR system is an example of an

enforceable accountability framework in which companies voluntarily adhere to codes of conduct to implement privacy protections across participating APEC economies.

Further, as part of ensuring the free flow of data, the law should prohibit data localisation requirements for both the public and private sectors. As discussed in the response to Chapter 9, such measures can frustrate efforts to implement security measures, impede business innovation, and limit services available to consumers.

BSA also urges the Government to refrain from imposing an adequacy requirement on international data transfers. An adequacy requirement is unnecessary under an accountability-based framework because of organizations' ongoing obligation to ensure appropriate processing. As such, accountability should remain the focus of data protection law.

Moreover, experience with the adequacy requirement in the EU's Data Protection Directive (which is also included in the GDPR) points to several significant drawbacks in instituting such a requirement. Adequacy reviews are time-consuming and burdensome, resulting in few adequacy findings. Adequacy reviews also focus heavily on formal legal standards, which may not provide a complete picture of the safeguards in a country. Conversely, the existence of formal legal protections in a country does not necessarily guarantee a high level of legal protection in practice. Finally, adequacy could limit the ability of companies in India to provide modern technologies and services. In short, an adequacy requirement is unlikely to add significantly to the level of data protection in India, but adequacy would likely hinder innovation and growth in India's digital economy.

Cross-Border Transfers of Sensitive Data

Some established mechanisms for transferring data, including the EU-U.S. Privacy Shield and Standard Contractual Clauses in the EU, have particular rules related to sensitive data, but the transfer of that data should be broadly permitted. A risk-based approach should be used to determine whether any additional safeguards should be imposed on the processing and transfer of sensitive data, as discussed in our response to Part III, Chapter 6. However, BSA strongly recommends against imposing bans on the transfer of certain categories of data, including based on the sensitivity of data.

In certain limited circumstances, such as those involving sensitive government data, we understand that restrictions already have been put in place in India. For example, currently under the "Request for Proposal for Provisional Empanelment of Cloud Service Providers" (RFP) issued by the Ministry for Electronics and Information Technology (MeitY), provisionally empaneled cloud service providers must guarantee that "all services acquired under this RFP including data will be guaranteed to reside in India". While it is understandable that certain types of government data may be subject to restrictions, the assessment should be based on specific factors, such as data sensitivity and likelihood of harm.

We understand that the Ministry of Home Affairs has developed manuals to classify data based on various factors, including sensitivity of the information, impact on India's national security, and strategic or administrative considerations. BSA submits that any such data classification exercise should be based on the principles

of transparency, predictability, and fairness and should be a clearly defined, publicly available, narrowly tailored, and easily administrable exception to the general rules governing international transfers. Otherwise, the prohibition could create uncertainty that slows the growth of Digital India.

Chapter 9 – Data Localisation
(Questions 1-2, 4)

As referenced in the response to Chapter 8, BSA does not recommend the adoption of data localisation requirements. This approach is consistent with developments in international trade agreements, which generally prohibit localisation requirements as a condition for doing business in a country. These agreements include limited exceptions for localisation measures necessary to achieve legitimate public policy objectives, provided they are no broader than necessary to achieve the objective and are not applied in a manner constituting a means of arbitrary or unjustifiable discrimination. Although important concerns about data protection, security, and law enforcement have led some countries to impose localisation requirements, they typically do not provide an effective means of addressing the underlying concerns and have significant negative consequences, including increasing costs to economies and local companies, limiting access to global services, and hindering innovation.

As the White Paper recognizes, data localisation measures have had a negative economic impact on GDP of several countries. (White Paper at 70.) For example, existing data localisation measures already have had an estimated -.8% impact on GDP in India, and an estimated 1.8% in Vietnam. It has also affected exports for several countries, resulting in a -1.7% export loss in both Indonesia and China. According to Gartner, public cloud services in India are projected to grow at 38% this year to total $1.81 billion. Data localisation requirements could impede this growth, as they often impose significant costs on the countries that adopt them.

Data localisation requirements also disproportionately impact small and medium-sized enterprises (SMEs) that do not have the resources to meet burdensome regulatory requirements. Access to digital products and services, such as cloud applications, provides SMEs with cutting edge services at competitive prices, enables them to participate in global supply chains and directly access customers in foreign markets. Indeed, the Internet is a great equalizer, enabling small companies to compete globally using the same tools as large and established companies.

Further, data localisation may prevent companies from offering services within a country, because it may be too costly or otherwise impractical to do so. Individuals have fewer and more expensive choices as a result. The White Paper cites studies showing that companies would be required to pay 30-60% more for their computing needs than if they could go outside the country's borders.

In addition, companies that are subject to data localisation requirements may not have unfettered access to innovations in other countries. This will hamper the development of domestic innovation that would otherwise occur by enabling local companies to access foreign cloud service platforms, analytics tools, and application programming interfaces (APIs). Further, data localisation can reduce the size of local

data sets, restricting the value that can be gained from cross-jurisdictional data consolidation and analysis. As a result, domestic companies would face higher costs, slower innovation, and isolation from customers in other markets. These effects could be most pronounced for India's start-up companies, many of which depend on access to low-cost cloud storage and computing services. As the White Paper acknowledges, many Indian start-ups forego making large capital investments in computer hardware and leverage cloud services to meet their business needs. (White Paper at 72-73.) In short, imposition of data localisation requirements would be contrary to the goals of promoting a "Digital India."

Chapter 10 – Allied Laws

The White Paper highlights the wide range of existing laws in India – including in the financial, information technology, telecommunications, and health sectors – that implicate the processing of data. We encourage the Government of India to ensure that any general data protection framework it develops supersedes any other legal requirements that apply to the protection of personal data so that a consistent approach can be developed that establishes clear rules, which will provide legal certainty for businesses of all sizes and help to facilitate compliance.

More generally, in light of the complexities of global compliance, the law should be applied in a manner that is consistent with international best practices to facilitate the ability of companies to provide products and services to Indian residents.

PART III: GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

Chapter 1 – Consent
(Questions 1-5)

Consent is an important basis for handling personal data. However, BSA urges the Government to recognize other legal bases for processing personal data, as discussed in our response to Part III, Chapter 4 of the White Paper. These additional bases for processing include the legitimate interest of companies handling the data, the performance of contracts with the data subject, and compliance with legal obligations. The data protection framework need not identify a primary ground for processing. Instead, legal grounds should be generally applicable, and it should be up to the data controller to determine the relevant ground(s) – and to ensure that its processing activities comport with such grounds.

The standard for determining the level of consent that is appropriate should be contextual. 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.

As the White Paper points out, it "is a questionable assumption" whether individuals can fully engage in privacy self-management through informed and rational decisions about data collection and use, given the vast number of instances of data collection in the modern world. A data protection framework that relies too heavily on individual consent will overwhelm individuals with decisions and render them unable to identify truly consequential decisions. This can lead to two further negative consequences: (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.

Recognition of implied consent can relieve some of this burden. The law could recognize implied consent for data processing associated with certain, specified purposes, such as fraud prevention and service fulfillment. The deployment of more data-intensive services in the future should also be allowed to rely on implied consent to collect personal data for processing that is not harmful, is reasonably expected, and allows services to operate. For instance, a public transportation service that uses electronic fare cards should not be required to obtain express consent each time an individual uses his or her card. Concerns about imbalances in bargaining power are less relevant in these kinds of cases, because the data processing poses little or no risk and directly benefits individuals.

Of course, 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.

Chapter 2 – Child's Consent
(Questions 1-4)

Special considerations are appropriate when the personal data of children is processed and, therefore, BSA supports efforts to protect children's privacy. To the extent an age limit is established to delineate when special protections should apply, we support identifying an age limit of 13, which is incorporated into US law, and is also the lower threshold that could apply under the EU GDPR. Establishing this age limit would extend protections to children during the age period that several governments have recognized is most vulnerable, promote harmonization with other privacy laws on this important issue, and facilitate compliance efforts for companies operating within multiple jurisdictions.

Chapter 3 – Notice
(Questions 1-7)

Consistent with our views on consent, BSA recommends that notice requirements reflect the context of data processing. When express consent is required, a clear and conspicuous notice that provides individuals with information relevant to their choice is appropriate. In other situations, a requirement to provide prominent notice is unlikely to advance privacy protections. Requirements that result in over-notification may result in individuals ignoring notices that are important for an express choice that they need to make.

Also consistent with the idea that notice should support choices that are contextual, the law should not prescribe the form or content of a privacy notice. Individuals are using an increasing number of devices from which personal data may be collected, and the displays on these devices are becoming smaller or even disappearing. Finding ways to provide effective notice in connection with such a diversity of devices is challenging, and prescriptive requirements in legislation are unlikely to address these challenges. Addressing this ongoing challenge should involve the input and efforts of industry, the Government, and other stakeholders. Because the issue of notice in a more connected, data-intensive world is unresolved, BSA cautions against prescribing specific means of presenting notice, such as a "consent dashboard." The specific requirements for this approach are not well understood. In the absence of prescriptive requirements, however, we do recognize that dashboards could be useful tools to promote user control.

While the drawbacks of presenting privacy notices separately from a device (*i.e.*, "decoupling" notice from the device) are real, this presentation may be the only means of presenting full and accurate information in a public document. Presenting privacy notices in this manner also affords the space and flexibility to offer translations in multiple languages, to reflect the diversity of individuals who use a product or service.

In addition, privacy impact assessments as proposed in the White Paper under this Chapter are not relevant in the context of notice and choice. Such assessments are conducted by organizations on their own processes to see how they might implicate the privacy of the individuals whose data they hold, collect or process. They are not applicable in the discussion relating to notification to individuals.

Finally, BSA does not support the use of a "data trust score" to encourage the development of effective notices. As presented in the White Paper, the data trust score concept only provokes further questions about how the score should be defined and what body should be responsible for providing it. It is unlikely that the quality of a notice – let alone a broader set of data practices – can be meaningfully boiled down to a single score. The effort and resources that would be required to develop a data trust score would divert resources of the government and businesses that would be better spent developing more substantive data protections.

Chapter 4 - Other Grounds of Processing

(Questions 1-4)

BSA supports providing multiple legal grounds for processing personal data. Consent is an important basis to offer, but it should not be the only legal basis for processing. As discussed below, other grounds of processing may provide a better fit for certain data processing situations. Consequently, these grounds may direct companies to consider requirements that are less burdensome for individuals and companies, while also resulting in more effective data protections.

Legitimate Interest

The legitimate interest legal basis for processing personal data, which is incorporated into many privacy laws around the world, is vital for enabling companies to conduct data processing that is necessary to carry out their business operations. Legitimate interest 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, businesses may need to handle personal data as part of network security or fraud prevention efforts. Seeking consent for such activities is not only impractical but may lead to harm to a significant number of individuals.

In addition, the law should recognize that companies may need to address user conduct that directly harms their interests. 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.

BSA recognizes that putting legitimate interest into practice not only requires the specification of additional factors to consider in determining whether it applies to an instance of data processing but also the exercise of judgment in each application. There are multiple ways to address this challenge. For example, the data protection framework itself could outline factors, based on further input and dialogue as the Government moves forward.

In the EU, for example, processing is permissible without the need for consent when it is necessary for the purposes of the legitimate interests pursued by the controller, except where those interests are outweighed by the impact of the processing on the rights of the data subject. The EU's Article 29 Working Party has outlined several factors for companies to consider in weighing data subjects' interests and applying this ground for processing.

The White Paper queries whether it is appropriate for data controllers to conduct the balancing test of individual rights that has been associated with the legitimate interest ground for processing. We note, however, that the data controller is obligated to assess and remediate data protection risks in a variety of circumstances under data protection laws, and they can exercise that judgment capably under these circumstances too. Several countries around the world have also recognized legitimate interest as an important basis for data transfers, including other non-EU countries within Europe, as well as South Africa. Other countries, such as Brazil, the Philippines, and Ghana, are considering legislation that would also recognize a legitimate interest ground for processing.

Finally, the concept of legitimate interest is embedded in a broader data protection framework. BSA emphasizes that accountability should be integral to this framework, and part of accountability is having the capacity to document decisions about data processing. Thus, an accountability-based approach provides important checks on the use of legitimate interest. And, of course, other rights and obligations under the framework, including various individual participation rights, will help ensure that data processing based on legitimate interest respects individuals' privacy rights.

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. For example, under Indian law, any organization that is affected by a cyber security incident must report the incident to the Indian Computer Emergency Response Team, "as early as possible," However, in the event of a large-scale incident affecting several users, it may not be practicable for the organization to obtain the consent of each individual user before complying with this legal obligation. The absence of any alternative grounds for processing would also hinder the ability of the organization and the relevant authorities to take swift corrective action. Therefore, 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.

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. These could include performing tasks in the public interest and protecting the vital interests of individuals, which are also recognized under other data protection laws. We recommend that the Government adopt a flexible approach that both protects individuals' privacy and preserves companies' ability to carry out their legitimate business operations and provide innovative services.

Chapter 5 - Purpose Specification and Use Limitation
(Questions 1-4)

BSA concurs with the White Paper's assessment that the "advent of newer technologies such as Big Data, data analytics and the Internet of Things may challenge the relevance of the purpose limitation, as it currently exists." (White Paper at 106.) Adopting a strict version of purpose specification and use limitation, which would require data to be collected for a specified purpose and used for no other purposes unless notice is given (and perhaps additional consent is obtained), could impose undue constraints on data processing and inhibit data-driven innovation.

As an alternative, BSA suggests permitting use for purposes that are compatible or related to the purpose for which data was collected, a standard that is also reflected in the APEC Privacy Framework, would be more consistent with new technologies and modern data-driven services. We note that several other elements of a data protection framework would provide ample protection under this modified purpose specification and use limitation principle. Accountable organizations will have processes in place to determine whether a reasonable relationship between initial and subsequent purposes exists, and they would document their decisions. Data security obligations would continue to apply to personal data that is used for related purposes. In addition, individual participation rights in the data protection framework, potentially including rights of confirmation, access, and rectification, would continue to apply. Finally, processing for additional purposes would require a satisfactory legal basis under the data protection law. Taken together, these elements of the data protection framework would provide robust safeguards for individuals and cause companies to make careful decisions about whether to process data for additional purposes.

Assessment of Compatibility

The data controller is in the best position to determine whether a subsequent use of data is reasonably related to the initial purpose. The criteria governing compatibility deserve more discussion as the Government develops its data protection framework, but the considerations should focus on context and individual expectations. For example, the law could require data controllers to consider whether the additional processing extends the initial purposes of collection and whether additional processing implicates greater sensitivity or risk. Data controllers might need to consider their relationship with individuals whose data is at issue and the circumstances under which the data was collected. For example, a company that registers users who use one of its services might wish to use the contact information that it collects in connection with the registration to notify users that additional services are available. Such a use of registration data is compatible with the purpose of initial collection and the relationship between the individual and the company.

BSA also suggests that the accountability-based outlook provides support for this kind of flexible approach. Accountable organizations will have appropriate processes in place to ensure that the organizations make and document well-reasoned decisions about whether additional purposes are reasonably related to the initial purpose of processing.

Role of Central and Sectoral Regulators

BSA recommends that the data protection law provide general standards to govern purpose specification and use limitation. This structure will provide a coherent framework to put these principles into practice. Many companies provide services in different industry sectors, and a general standard would enable them to achieve a more consistent application of the data protection framework. Such consistency can be accomplished by consolidating data protection oversight in one central regulator with broad understanding of different industry sectors, rather than bifurcating the regulation amongst several regulators.

Chapter 6 - Processing of Sensitive Personal Data

(Questions 1-4)

BSA recognizes that cultural and socio-economic considerations may counsel that certain types of data be deemed sensitive, and that those categories, as defined in other data protection laws, often include racial or ethnic origin, political opinions, religious beliefs, genetic or biometric data, health information, or information regarding sexual orientation. However, even if the Government designates these categories of information as sensitive, BSA supports a risk-based approach to determine whether heightened protections should apply to sensitive data.

Fundamental to the risk-based view is the notion that not all personal data is the same, nor are all data processing activities the same, in terms of the risk that they pose to individuals. BSA suggests that meaningful distinctions among personal data types must begin with an identification of concrete, specific, and measurable harms. This harm-based outlook will help keep sensitive data classifications, and any relevant processing restrictions, confined to cases in which the processing of sensitive personal data poses a potential to cause significant harm to individuals.

In practice, the use of personal data is often as important to determining whether there is heightened risk to the individual. Modern devices and services generate and use a large volume and variety of personal data, but little of this data, on its own, presents a risk of concrete, specific, measurable harm to individuals. An effort to determine whether such data is sensitive is likely to go astray. Examining risks arising from the *use* of data, by contrast, would direct the focus of companies toward reducing risk in the context of their own data processing operations. For example, certain types of information implicate clear privacy interests to the individual. However, it is still appropriate to apply a risk-based approach. For example, if sensitive personal data is used by an employer to process employee benefits to comply with relevant laws, the risk of harm is lower to the individual than it otherwise would be in the context of a public disclosure and, therefore, should not be subject to the same requirements.

More generally, this risk-based focus will lead to greater flexibility in data processing and promote innovative uses of data while also providing appropriate data protections. Risk-based data protections will be more effective in identifying and mitigating new or emerging risks than will static processing requirements (or restrictions) based on data sensitivity.

Accordingly, BSA recommends keeping the data protection framework focused on risk, including with respect to sensitive data, and applying protections where there is a risk of concrete, specific, and measurable harm to individuals.

Chapter 7 - Storage Limitation and Data Quality
(Questions 1, 3-4)

BSA supports a storage limitation standard that permits companies to store personal data for as long as it is relevant to the purposes for which it was collected. A specific, quantitative limitation on the data retention period is not workable because of the vast diversity in the data processing operations that are necessary to support modern data-driven services. For example, any attempt by the Government to prescribe storage limitation standards, based on duration, manner and format, as provided for under Section 67C of the Information Technology Act, 2000, would be difficult to implement given the wide variety of services and data categories that would fall under its ambit. Similarly, a qualitative standard that is too strict will inevitably require companies to delete or anonymize personal data before it provides its full value to individuals.

Other data protection mechanisms are better suited to ensuring that companies do not retain personal data that is no longer relevant. Companies identify (or refrain from collecting) data that is not relevant to their processing operations through their accountability programs. Data security programs help to protect all personal data under a company's control from unauthorized disclosure and use. Anonymization also protects data from misuse and misappropriation.

BSA's proposal to permit personal data storage for as long as data is relevant to the purposes for which it was collected avoids the pitfall of a specific, one-size-fits-all rule for deletion or anonymisation. This standard would give companies the flexibility to provide innovative data-driven services while ensuring that they remain responsible for deleting or anonymising personal data that is no longer relevant. Other data protection processes, including ensuring that data collected is relevant to specific purposes and maintaining data security programs, also provide effective safeguards.

Chapter 8 - Individual Participation Rights – 1
(Questions 1-6)

It is critical to strike the right balance between the scope of confirmation, access, and rectification rights with the potential legal effects of data processing. The legal effects of data processing vary widely with context. Some data processing leads to significant decisions (*e.g.*, employment and credit) by persons other than the individual, which can have a significant impact on the individual. Other instances of data processing might only affect or influence choices that individuals make, such as which item to purchase online. In these contexts, the individual remains the decision-maker. These two contexts raise substantially different issues with respect to individual participation, and confirmation, access, and rectification rights should take these differences into account.

BSA suggests requiring companies to respond to an individuals' request for confirmation, access, and rectification *without unreasonable delay*, rather than under a fixed timeline. A single time period cannot take account of the widely varying complexity in companies' data processing systems and operations. As the White Paper notes, some data controllers hold large volumes of unstructured data (such as

email) (White Paper at 124), and extracting information about specific individuals is, at best, challenging.

Moreover, setting a fixed timeline implies that all needs behind confirmation, access, and rectification are equal. As discussed above, they are not. Considerations for setting a standard to respond to individual requests should take into account the impact of data processing on the individual as well as whether the individual is the relevant decision-maker. We also note that requiring a reasonable fee would be consistent with approaches in other countries, and it would also enable resources to be spent on more specific, individualized attention to these requests.

The implementation of the access principle is more complex in the context of automated systems. BSA members understand the importance of raising awareness about how such systems operate, and they are undergoing efforts to do so. We note, however, that this is an area of ongoing research and study. As discussed in the response to Chapter 9, imposing prescriptive rules about how companies provide relevant information about those systems would be premature.

Chapter 9 - Individual Participation Rights – 2
(Questions 1, 3-4)

BSA strongly supports giving individuals more control over their data. At the same time, any additional individual rights under a data protection framework should be consistent with the goal of harnessing the benefits of the digital economy. (*See* White Paper at 4.) To that end, it is essential that the law establishes requirements that are technically and commercially reasonable to implement and does not prescribe how they must be implemented.

Restriction of Processing

Creating an independent right to restrict personal data processing would be inconsistent with the objectives of harnessing the benefits of the digital economy while fully protecting individual privacy interests. As it is described in the White Paper, a right to restrict processing would provide "temporary relief" while an individual challenges the accuracy or relevance of data, the legality of processing, or pursues an objection to processing. In short, this right would short-circuit the processes that are called for to make determinations about the legality of data processing or the exercise of other individual rights. A general obligation to comply with requests under this right would be highly disruptive to businesses. It would also disrupt the balance that is established through rights such as accuracy and relevance, by essentially requiring companies to presume that all challenges under such rights should be resolved in favor of the individual.

Objection to Automated Decision-Making

The White Paper highlights certain implications of automated decision-making, opines that legislation elsewhere addressing this issue lacks sufficient safeguards, and considers creating a "practically enforceable and effective right." (White Paper at 130, 133, and 135.) BSA acknowledges that various issues could arise in the context of automated decision-making. However, because this is an area where technology continues to evolve, we emphasize that prescriptive rules could both frustrate innovation and fail to achieve the aim of creating a framework that is

"practically enforceable and effective." We note further that this continues to be an area of considerable research, including on how these emerging technologies could be used to detect and address bias.

If the Government considers implementing a right to object to automated decision-making at this stage, the scope of that right should be clearly defined, and it should be targeted to address the particular harms that could arise. To that end, BSA recommends that the law avoid adopting an overbroad approach, such as one that would impose a blanket prohibition on automated decision-making processes, and that any restrictions be limited in two important ways. First, a right to object should apply only in circumstances where the decision-making is based *solely* on automated-decision making. In circumstances where humans play a role in reviewing the information and participating in the decision, even where the reviewer receives initial input from an automated process, the restrictions should not apply, as the human participation provides an appropriate safeguard against potential harms.

Second, the right to object should be limited to decisions based solely on automated decision-making that can have significant legal or economic consequences, and where the other rights and obligations in the framework are insufficient to guarantee protection of the individual's interests. Otherwise, a right to object to automated decisions could override the structure of rights and obligations established elsewhere in the data protection framework. Limiting a right to object to decisions with significant legal and economic consequences, such as access to employment, housing, or credit, rather than expanding it to include areas that simply provide information for consumers to make informed decisions, such as advertising, would both carefully tailor it to instances in which there is a substantial risk of harm and enable the application of objective criteria to ensure that the right is practically enforceable.

Chapter 10 - Individual Participation Rights – 3: Right to Be Forgotten
(Questions 1, 3-6)

BSA supports the aim of giving individuals choice and control over their data. The consent and individual participation rights, the storage limitation obligations, and other rights and obligations discussed in the White Paper can help achieve this objective. We understand that the Karanataka High Court, in *Sri Vasunathan v. The Registrar General*, recognized a "right to be forgotten" in connection with highly sensitive information, and that the Supreme Court of India, in the *Puttaswamy* case, further acknowledged how the ability to delete information online can impact privacy. As the Government assesses how to incorporate these concepts into a data protection framework, BSA outlines below how such a right might be applied and identifies three important factors to consider in shaping deletion rights—clearly defining the scope of any such rights, ensuring the balancing of other rights, and creating a practical framework that is reasonable and practicable.

As the White Paper recognizes, courts in some jurisdictions, including the EU and Japan, have applied what is commonly known as the "right to be forgotten" with respect to online search results. BSA appreciates the concerns of protecting individuals' privacy online. We also recognize that unqualified extensions of this right, particularly if defined and applied inconsistently across multiple jurisdictions, could hamper efforts to develop pragmatic, effective solutions to protect privacy and

negatively affect the larger Internet ecosystem. Therefore, certain options – such as the possibility of extending such a right into the physical space, or extending the right beyond delinking of online information – must be assessed in a balanced and practicable manner, as emphasized by the Supreme Court in *Puttuswamy*.

As a result, BSA recommends that any "right to be forgotten" be limited as it has been applied in the EU, including applying exclusively to data controllers operating online search engines, since this is the context in which courts have articulated the right and is most closely tied to the individual interest in ensuring that certain types of information remain obscure. We recommend that the available remedy should be limited to blocking of certain results that appear upon a search of the requester's name, but the underlying link and content should still otherwise be searchable. This would strike a more appropriate balance among varied individual rights and interests.

More generally, we also highlight three key considerations for defining deletion rights.

First, the right should be carefully tailored to circumstances where the personal data is no longer necessary for the purpose it was collected, the data subject has withdrawn consent and no other legal ground exists to the process the data, the data pertains to a child under the age of 13, or the data has been unlawfully processed.

Second, as the White Paper recognizes, it is vital that any requests to delete personal data be balanced with other important rights, such as freedom of expression. In addition, the law should also recognize other circumstances where the exercise of such a right may not be appropriate, such as compliance with a legal obligation or defense of legal claims, for public interest reasons, including public health, or for scientific or historical research purposes.

Finally, any obligations associated with this right should require only that data controllers make technologically and commercially reasonable efforts to delete data that is implicated by an individual's deletion request.

Part IV: Regulation and Enforcement

Chapter 2 - Accountability and Enforcement Tools
(Questions 1-7)

BSA supports the use of the principle of accountability in the Government's data protection framework, provided that the focus of accountability in practice is on the outcomes of data processing, rather than prescriptive ex ante requirements and administrative processes that add little to the objective of increased data protection.

Accountability is best implemented through its underlying components, rather than as an additional, distinct legal obligation. The accountability model established under the OECD *Guidelines Governing the Protection and Transborder Flows of Personal Data* and other frameworks focuses on establishing the responsibility of the data controller for personal data protection, no matter where or by whom it is processed. The White Paper discusses several data protection elements that would advance this holistic conception of accountability. For example, appropriate data

security measures are integral to an ongoing process of data protection. The use of processes such as Privacy by Design can also provide an effective means of protecting personal data throughout the data lifecycle. However, we emphasize that Privacy by Design is a process, and the specifics of any such process will vary with the kind of organization involved, the nature of its data processing operations, and other factors. Relatedly, the risks arising from data processing vary with the specifics of its operations, as do the appropriate safeguards and mitigations. Companies need the flexibility to carry out these processes in a way that fits their operations. Finally, the totality of a company's efforts to protect personal data should be taken into account in any sanctions that are imposed for alleged violations of the law, as discussed in our responses to the questions in Chapters 4A-4C.

Any incorporation of accountability in the Government's data protection law should also avoid creating uncertainty about the responsibilities and liabilities of the entities involved in data processing. As discussed in our response to Chapter 6, clearly assigning primary responsibility for compliance to the data controller is critical and ensures that the increasingly widespread practice of outsourcing does not create 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.

BSA opposes strict liability standards in data protection laws. In particular, imposing civil penalties under a strict liability standard would create excessive deterrence, leading to less innovation and higher costs for products and services. Moreover, 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 impact on potential investments in data processing and outsourcing services. Contracts between data processors and data controllers are sufficient to ensure that data processors comply with data controller instructions and to ensure the security of the data they process.

Finally, BSA urges the Government to refrain from adopting any insurance requirements in connection with liability under the data protection law. Clarity in the law about the allocation of liability and the range of potential monetary liability will provide the basis for companies to make their own decisions about the need for insurance.

Chapter 2A - Codes of Practice
(Questions 1-6)

Codes of practice can substantially advance the goals of data protection. In particular, codes of practice can provide additional guidance to companies as they design, implement, and maintain data protection programs. Developing and implementing codes of practice, however, requires the commitment of significant resources. The law should recognize the beneficial roles that voluntary, industry-led, consensus-based codes of practice can play and create appropriate incentives to develop and adopt them; but the law should not require businesses to use codes.

BSA supports public-private collaboration under the umbrella of an industry-led, voluntary, consensus-based process. Industry leadership is a critical element in the successful development of codes of practice. The entities that process personal

data are deeply familiar with the many technical, business, and compliance facets of modern data processing, and this familiarity is a critical part of producing codes of practice that both protect personal data and are reasonable to implement. Government and other stakeholders also may have insights that can improve codes of practice, and their participation in code development should be encouraged.

The APEC CBPR system provides an example of the successful public-private sector collaboration to develop of a data protection code of practice. Although APEC economies led CBPR development, they drew significant input and assistance from industry. The result is a voluntary, accountability-based set of program requirements that facilitate privacy-protecting cross-border data flows and are enforceable in APEC economies. The object of the CBPR – facilitating data flows among a group of large, dynamic economies – illustrates the kind of value that can justify the commitment of resources necessary to produce a code of practice.

The International Organization for Standardization's (ISO) voluntary, consensus-based, multi-stakeholder framework for development of standards is another example of how codes of practice can be developed and used to enhance data protection. For example, ISO/IEC 27000's family of standards help organizations strengthen information security management systems, and ISO/IEC standard 27018 establishes a code of practice for protecting personally identifiable information in public cloud services, which companies, including some BSA members, implement to enhance cloud security.

In India, codes of practice have been used in different sectors, including the media and advertising sector. For example, the "Code for Self-Regulation in Advertising" developed by the Advertising Standards Council of India (ASCI) serves as the principal framework for advertisers to demonstrate compliance with existing advertisement laws. The ASCI code functions as a voluntary, self-regulatory mechanism, and it is recognized as a successful industry-driven effort that is currently being used in India. BSA recommends that a similar approach may be followed in developing suitable codes of practice in the context of a data protection framework for India.

In short, codes of practices are important components of data protection frameworks, and BSA recommends that the Government facilitate their use as voluntary mechanisms for organizations to demonstrate compliance with legal obligations, including in the context of cross-border data transfers.

Chapter 2B - Personal Data Breach Notification

(Questions 1-6)

BSA supports reasonable and appropriate personal breach notification requirements. 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. Requiring notification only when there is a ***material risk of harm*** to affected individuals would serve this goal.

To prevent or mitigate harm to individuals as the result of a breach, the foremost priority of the affected entity should be to stop or contain the breach, and fix the vulnerability or error that caused it. To this end, it is critical to allow these entities

sufficient time to conduct a thorough investigation of a security incident once they become aware of it. This allowance is necessary to determine the scope and impact of the incident and any breach of personal data, and to prevent further disclosures. BSA recommends 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 to affected individuals and/or data protection authorities.

Moreover, the data protection framework should recognize 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. Requiring notification only when there is a material risk of harm focuses on breaches that individuals need to know about in order to protect themselves. A breach involving information that permits access to financial accounts is perhaps the clearest example of material risk of harm to individuals. A focus on breaches with material risk also provides clarity as to the information that should be included in individual notifications. For example, information about affected financial accounts and specific steps that individuals can take to secure their accounts and prevent misuse of data exposed in the breach would be important to communicate.

The material risk standard would largely 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. Notification in the absence of such risks may create “notification fatigue,” leading to undue inconvenience for individuals as well as the possibility that individuals will fail to take appropriate action in response to notifications that indicate a real risk of harm.

Furthermore, a personal data breach notification system should also exclude from the notification obligation all instances in which 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).

Finally, the Government should consider the allocation of responsibilities between data controllers and data processors. Data controllers typically hold a direct relationship with the individuals whose data is involved in a breach. Therefore, it is generally more appropriate and efficient for the data controller to be responsible for providing notification of a breach. When a data processor suffers a breach, it should be required to notify the relevant data controller (in addition to taking any other steps required in the terms of their contract), but the data controller should remain responsible for notifying affected individuals. For example, if a data processor that stores purchase histories on behalf of a retailer experiences a breach, notification by the retailer – which holds a direct relationship with affected individuals – will be more meaningful and effective than notification by the processor.

Chapter 2C - Categorisation of Data Controllers

(Questions 1-5; Registration Questions 1-2; Data Protection Impact Assessments Questions 1-3; Data Protection Audit Questions 1-5; Data Protection Officer Questions 1-2)

BSA sees little to gain from establishing different categories for data controllers based on, for example, the harm that they may cause to individuals through data processing. BSA supports a risk-based data protection framework, and

risk should guide both the content of companies' obligations under the law as well as their decisions about how to implement the law's requirements. Attention to risk, combined with processes that provide organizational accountability, would require companies to engage in an ongoing process of assessing and mitigating their data processing risks. Categorizing data controllers would add little to these efforts.

Moreover, the creation of data controller categories could create unintended, adverse consequences for individuals and the economy. Many companies in the modern, data-driven economy handle a wide diversity of personal data and engage in a broad range of data processing. Requiring data controllers to fit within specific categories could disrupt the efficiencies of having these different operations under a single set of data systems and data protection processes. There is also a risk that data controller categories would be under-inclusive or over-inclusive. This, in turn, could lead to under-protection of data, or an unduly high level of protection. All of these outcomes would reduce companies' flexibility and could impede innovation while providing no data protection benefit.

Registration

BSA is opposed to any registration requirement for data controllers. Identifying and addressing risks based on the nature or volume of personal data that a controller processes should be integral to the controller's data protection processes. The framework discussed in the White Paper also makes consideration of risk key to the elements of a data protection law that the Paper discusses. Creating a registration requirement is unlikely to add meaningfully to companies' awareness of risk. Instead, registration will mainly serve to create additional compliance costs for companies as well as burdens for the regulatory or enforcement authority.

Data Protection Impact Assessment

BSA supports an accountability-based approach to data protection. At the same time, we favor providing businesses with the flexibility to implement processes that make sense in the context of their data processing operations. An assessment prior to undertaking high-risk processing, as discussed in the White Paper (at p. 168) may be a useful tool within a set of accountability processes. However, making this assessment mandatory is unnecessary and likely to lead to additional prescriptions about the form and content of the assessment, all of which will add to the compliance burden and reduce flexibility.

Data Protection Audit

BSA acknowledges that voluntary audits conducted for internal accountability purposes may be useful, but we do not recommend making data protection audits mandatory. Data processing and data protection are fundamentally dynamic endeavors. BSA members already provide broad process-based data governance and technical controls to ensure that they are handling and using data appropriately. These processes can be helpful to understanding a data protection program's effectiveness and whether any adjustments are warranted.

Adding a legal requirement to conduct audits would impose significant additional cost and inflexibility while creating few, if any, benefits for data protection.

Similarly, granting a data protection authority the legal authority to conduct audits would disrupt companies' operations and divert resources from areas in which they add more meaningfully to data protection.

Data Protection Officer

BSA supports incentives to encourage the appointment of data protection officers (DPOs) and understands that other specific officers, such as a Grievance Officer, are required under other laws in India, but we recommend against instituting a mandatory requirement. Organizations vary tremendously in staff, structure, and resources. Small and medium-sized companies might not have the resources to comply with a prescriptive DPO requirement. For companies operating in several countries, this function is often a global one, and it should not be mandated as a national role. In addition, some of the functions that the White Paper discusses in connection with DPOs may be difficult to fill with a single officer. For example, the White Paper suggests that a DPO "facilitate compliance" and "act as a point of contact with a data protection authority." (White Paper at 170.) Executing these duties effectively requires quite different skills; understanding data protection requirements and how to implement them involves a much different body of knowledge than interfacing with a government enforcement official. Both functions are important to data protection, but it might be impractical to expect one official to be responsible for them. A better course may be to ensure that the framework's requirements, as a whole, provide an appropriate level of accountability, and leave it to companies to determine how best to meet those requirements.

Chapter 2D - Data Protection Authority
(Question 1)

Effective enforcement by a data protection authority is an important element of any data protection framework. At the same time, transparency, predictability, and fairness during any investigation and adjudication are critical from the perspective of companies that strive to comply with the law and respond to any investigation. Such a body should be a central authority (i.e. not federated) and should not be directly financed by income from penalties, so as to avoid the potential for or appearance of bias in decision-making. In addition, several jurisdictions have recognized the importance of having an independent agency enforce data protection laws, including in the EU and Canada, and this may also be an issue that the Expert Committee should consider. BSA would welcome the opportunity to comment further on issues relating to a data protection authority once additional details of India's data protection framework are available

Chapter 3 - Adjudication Process
(Questions 1-2)

BSA would welcome the opportunity to engage further on the details of adjudication processes as more specifics of the data protection framework are developed. However, at this stage, we point out that there are significant downsides to requiring enforcement authorities to become involved in resolving individual disputes. This level of involvement requires a large commitment of resources, which might be better spent investigating significant or large-scale violations of data protection law. In the United States, for example, the Federal Trade Commission

does not resolve individual consumer complaints, focusing instead on strategically selected enforcement actions that address harm to large numbers of consumers, shape industry norms, or stop especially harmful practices.

Chapter 4A – Penalties
(Questions 1-6, 11)

Fair and reasonable civil penalties can add credibility to data protection law and deter violations. Therefore, civil penalties are a potentially useful data protection enforcement tool.

However, civil penalties should be available only for willful or manifestly negligent violations of legal requirements. Data protection enforcement should focus on accountable practices, increased detection, and the promotion of feedback or guidance to improve operational practices. Imposing civil penalties under a strict liability standard would create excessive deterrence, leading to less innovation and higher costs for products and services. Civil penalties also should not become the primary enforcement objective, nor should they be used to threaten data controllers and data processors that act in an accountable manner.

The law should provide additional safeguards in connection with civil penalties. Most importantly, the law should not link civil penalties to a percentage of a company's worldwide turnover. Using worldwide turnover to calculate a civil penalty has the effect of imposing a global sanction, which in turn may punish a group of companies for the actions of a single subsidiary. This type of penalty is at odds with fair and reasonable enforcement and could deter further investment in India.

In addition, the law should require the data protection authority to consider the circumstances – and mitigating factors – surrounding each alleged violation. Specifically, if alternative remedies, such as imposing additional requirements on a specific company's processing activities following a full investigation, would address the violation, then the law should direct the data protection to use that remedy.

Finally, the level of civil penalties should be tied to any additional programs or processes that a company puts in place after a violation. These remedies should be designed to prevent future violations and therefore reduce the need to rely on civil penalties for deterrence.

Chapter 4C – Offences
(Question 1)

BSA opposes the creation of criminal liability for violations of data protection law. The substantive requirements of data protection law, combined with monetary relief and conduct remedies provided through administrative or civil judicial processes, are sufficient to protect individuals' privacy interests.

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 OECD[1] 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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.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