MORRISON | FOERSTER

250 WEST 55TH STREET
NEW YORK, NY 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON & FOERSTER LLP

BEIJING, BERLIN, BRUSSELS,
DENVER, HONG KONG, LONDON,
LOS ANGELES, NEW YORK,
NORTHERN VIRGINIA, PALO ALTO,
SAN DIEGO, SAN FRANCISCO, SHANGH
SINGAPORE, TOKYO, WASHINGTON, D.

February 24, 2020

Writer's Direct Contact
+1 (212) 506.7213
MWugmeister@mofo.com

# GLOBAL PRIVACY ALLIANCE COMMENTS ON INDIA'S PERSONAL DATA PROTECTION BILL, 2019

We write on behalf of the Global Privacy Alliance (GPA). We welcome the opportunity to submit comments in connection with the Indian parliament's public consultation on the Personal Data Protection Bill, 2019.

The GPA is comprised of a cross section of global businesses from the automobile, aerospace, communications, computer and computer software, consumer products, electronic commerce, financial services, logistics, and travel/tourism sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

## KEY RECOMMENDATIONS

### Processing of Foreign Data

- Personal data that are originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, and sent to India for further processing should be exempt from the application of the Act. Application of Indian privacy rules to the processing of such data in India would impose an additional layer of regulation on such processing that would discourage the use of India-based service providers. Moreover, an Indian service provider should be able to return data to its customer outside of India without adding additional regulatory obligations.

### Cross-Border Transfer Rules

- Transfers should be permitted on the basis of a contract, intra-group scheme, an adequacy decision, DPA authorization, compliance with a legal obligation, legitimate interests/reasonable purposes (such as those in Article 14 of the Act)] *or* consent. Consent should not be an additional requirement when transferring on the basis of a

contract, intra-group scheme, adequacy decision, DPA authorization, compliance with a legal obligation, or legitimate interests/reasonable purposes.

**Data Localization**

- Data localization has a negative impact on businesses that rely on cross-border data transfers to provide services to customers in India and disrupts the provision of such services. Data localization would reduce the ease of doing business in India, because data-reliant companies would not be able to transfer data easily to affiliated companies or business partners or service providers outside India.

**Data Breach Notification**

- The current definition of harm under the Act establishes a very low threshold for triggering notifications, one that is likely to result in over-notifying and desensitizing individuals and inundating and overwhelming the data protection authority. To avoid these problems, the Act should provide for a reasonable and balanced notification trigger that ensures that individuals receive notice when there is a significant risk of substantial harm.
- The Act should specify the sensitive information that would be subject to notification obligations.

**Penalties**

- The penalties proposed under the Act are excessive and may restrict economic activity and growth. We recommend that criminal penalties be eliminated from the Act because they are likely to have a chilling and deterrent effect on business entry into the Indian marketplace.

**Transition Period**

- We recommend that specific language regarding an adequate transition time be added, for example, a minimum timeframe of 24-36 months similar to the transition period under the EU General Data Protection Regulation ("GDPR").

## ADDITIONAL RECOMMENDATIONS

**Legal Bases: Processing Data for Reasonable Purposes and Employment Purposes**

- The trend in data protection law, as evidenced by the GDPR provisions, is to move away from relying on consent as a primary legal basis for processing and providing reasonable exceptions to the consent requirements for uses of data that consumers would reasonably expect to occur. Over reliance on consent results in individuals experiencing consent fatigue (i.e. individuals simply click yes without reading the underlying information) and adds a substantial cost burden on organizations without adding privacy protections for individuals. Therefore, the Act should provide for these additional exceptions and/or clarify:

- The Act should provide an additional exception for processing that is necessary to fulfill contractual obligations. This legal basis is recognized in the GDPR and in most other privacy laws around the world.
- The Act should include an exception for processing that is in the data fiduciary's legitimate interests where not outweighed by the impact to the individual. This legal basis is recognized in the GDPR and many other privacy laws around the world.
- The Act should make explicit that processing necessary for information security purposes and to prevent, detect, monitor, and control fraud, cybercrime, bribery, money laundering, and terrorism constitutes processing for a reasonable purpose.
- In connection with processing for employment purposes, all personal data, including sensitive personal data, should be covered by the provisions in Article 13. Employers often need to process sensitive personal data (as defined under the Act) such as financial data, selected health data, and official identifiers for payroll purposes and provision of benefits such as insurance. In addition, the Act should provide exceptions for: conducting internal investigations into suspected wrongdoings; enforcing internal company policies; and deploying monitoring technologies in the workplace for network and information security purposes (e.g., Data Loss Prevention).

**Data Audit & Trust Scores**

- The external audit requirement in Article 29(1) should be modified to permit organizations to carry out either internal or external audits, depending on their in-house capabilities. Many large companies have robust internal audit units that are sufficiently independent (e.g., they report to the compliance department rather than a specific business unit and/or report directly to the company's Board of Directors). Forcing all organizations to hire external auditors, regardless of their in-house capabilities, imposes unnecessary costs and exceeds requirements under other global privacy regulations. In addition, organizations that are regularly reviewed by regulatory authorities should be exempted from any specific audit requirements.
- Moreover, the requirement for the data auditor to assign a "Trust Score" should be removed because assigning a Trust Score is not a standard practice globally and may cause undue biases and unscientific score comparability.

**Data Protection Impact Assessments (DPIAs)**

- The DPIA requirement should be limited be to processing that poses a "serious risk of negative and unknown consequences to privacy". Imposing a lower standard – one that triggers DPIAs for processing that is not high risk -- is overly burdensome, costly, and unnecessary.
- DPIAs submitted to the Authority should not be made public. To do otherwise will discourage their use and possibly compromise the integrity of the assessment itself and the overall security of the product or service. Their value as a powerful internal

tool enabling organizations to manage and mitigate their risks would be severely undermined. Organizations that do carry out such assessments should maintain appropriate records that can be inspected by authorities in the event of a compliance or enforcement investigation.

**Data Protection Officers**

- A data fiduciary should be permitted to select its DPO based on qualifications and organizational structure rather than physical location.

**Complaint Handling**

- The Act should provide for a more reasonable time period for data fiduciaries to resolve complaints. Complaints often take time to resolve. Instead, it would be more reasonable to require organizations to respond to complaints within 30 days without mandating a specific timeframe for resolution of any grievances.

**Anonymized and Non-Personal Data**

- The Act grants the government the power to "direct any data fiduciary or data processor to provide any personal data anonymized or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government." This language could potentially include confidential, proprietary, or trade secret information of data fiduciaries, even if processed or stored outside of India. We recommend that the language be clarified that such non-personal or anonymized data must be actually used by a data fiduciary to provide services to individuals in India. This would also support the Act's goal "to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government."

## DISCUSSION OF KEY ISSUES

### 1. Application of the Act (Article 2(A)(c)(i))

***Processing of Foreign Data.*** The Act applies to all personal data processed within India. It would cover personal data that are originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, and sent to India for further processing. Because many organizations outside of India rely on Indian-based companies to process their foreign personal data, application of Indian privacy rules to the processing of such data in India would impose an additional layer of regulation on such processing that would discourage the use of India-based service providers.

We urge, therefore, that the government make explicit in the Act that the aforementioned foreign data are exempt from the application of the Act. This is the approach used by the Philippines in its data privacy law. We think this is a sensible approach and one that will

reassure Indian outsourcing service providers and their clients that the Act will not disrupt their outsourcing activities by adding another and possibly conflicting layer of regulation.[1]

***Extraterritorial Application.*** We recommend that Section 2(A)(c)(i) be edited as follows: "in connection with ~~**any business carried on in India, or**~~ any systematic activity of offering goods or services to data principals within the territory of India". The original language makes the extraterritorial application too broad (broader than the GDPR).

**2. Data Localization and Restrictions on Cross-Border Transfer of Sensitive Personal Data (Articles 33-34)**

***Data Localization.*** Article 33(1) requires sensitive personal data to be stored in India. In addition, Article 33(2) enables the government to identify categories of personal data as critical data that must be processed solely in India. Imposing such data localization requirements is detrimental to companies, citizens and the country's economy for the following reasons.

Local Storage Requirement

- Data localization would significantly increase costs since businesses would no longer be able to rely on economies of scale for data storage at global data centers, making services more expensive for customers. Companies that rely on cloud storage would have to radically overhaul their business models.
- Data localization requirements increase security risk and reduce data minimization efforts. Allowing companies to store data centrally facilitates better and stronger protection than if data are required to be stored locally.

Prohibitions on Processing Certain Categories of Personal Data outside of India

- Data localization has a negative impact on businesses that rely on cross-border data transfers to provide services to customers in India and disrupts the provision of such services.
- Data localization would reduce the ease of doing business in India, because data-reliant companies would not be able to transfer data easily to affiliated companies or business partners or service providers outside India.
- The development of technologies such as internet of things, artificial intelligence and machine learning would also be hindered because cloud computing and seamless data transfers are necessary for such technologies to operate. It will also affect start-ups

[1] See Section 4 of the Data Privacy Act of 2012, available at http://www.gov.ph/2012/08/15/republic-act-no-10173. In particular, Section 4 states: " This Act does not apply to …(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines."

and innovative new businesses from taking off as it would increase their cost of operations.

- Data transfers represent a key component of India's economy. Several studies indicate that data localization adversely affects the GDP of the country.[2]
- From a policy standpoint, if other countries were to adopt similar data localization rules, it would be harmful to India's outsourcing economy as data would not be able to be stored in India.

For the above reasons, data localization requirements for sensitive personal data should not be mandated in India. If India does opt to introduce data localization requirements, they should be limited to Government data, which, if disclosed, would harm national security, sovereignty, friendly relations with foreign states, or legitimate public interest (Sensitive Government Data). This includes data about the military, Government cybersecurity systems, classified documents, etc. An example of this approach to data-classification is set out in the National Data Sharing and Accessibility Policy, 2012, which classifies Government data as shareable and non-shareable and does not allow sensitive data, as defined by Government departments and organizations, to be shared. Under the data protection law, sectoral regulators should create a list of Sensitive Government Data which would be subject to localization requirements.

Moreover, any data localization provisions should make clear that they do not apply to the processing of personal data, including sensitive personal data, of individuals not within the territory of India.

***Cross-Border Transfer Rules.*** Article 34 sets forth the conditions under which sensitive personal data may be transferred outside of India. In particular, two conditions must be satisfied to carry out such transfers: 1) individuals must give their explicit consent to the transfer; and 2) the transfer is based on DPA-approved contracts or intra-group schemes, the transfer is to a country recognized by the DPA as providing adequate protection, or the transfer is necessary for specific purposes pre-authorized by the DPA.

This requirement exceeds the cross-border transfer requirements in virtually all of the data protection laws around the world that impose such restrictions, including the EU GDPR. Transfers should be permitted on the basis of contractual clauses, intra-group transfers, adequacy, DPA authorization, contractual necessity, legitimate interests/reasonable purposes (such as those in Article 14 of the Bill), *or* consent. There will be situations in which a data fiduciary in India does not have an existing relationship

[2] For example, see *Regulating For a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia* by J. Meltzer and P. Lovelock (March 2018), available at https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf.

with a data fiduciary in another jurisdiction but has been instructed by a customer or employee to make that transfer. For example, a customer instructs the organization to forward his or her financial information to his or her accountant or the organization forwards information to the immigration authorities so that a potential employee can be granted a work visa. In these examples, entering into a contract is impractical because there is no on-going relationship between the data fiduciary and the third party to whom the information is disclosed. In each of those instances, the data fiduciary should be able to transfer the data solely on the basis of the individual's consent.

Moreover, with respect to DPA-approved contracts, the Act should specify what provisions should be included in a contract rather than either requiring the use of form contracts or the need for DPA approval for individual contracts. This would be a similar approach as taken by several other countries, including the EU in the GDPR Article 28, in which the law lays out the provisions that should be contained in contracts rather than requiring approval or the use of form agreements.

**3. Definition (Article 3)**

***Personal Data.*** The definition of personal data currently includes inferred data. We recommend that the definition be clarified to make clear that inferred data can be personal data only to the extent that such data are linked to an identifiable individual.

***Sensitive Personal Data.*** We recommend that financial data, which are often regulated under the laws specific to financial institutions, not be included in the definition because such data are generally not considered to be sensitive information in most privacy laws around the world. Financial data can cover a wide array of information (e.g., bank name, account type, balance) but individually, these data are not sensitive per se. Most data protection laws, including the GDPR, do not include financial information in their definition of sensitive personal data.

***Harm.*** The definition of "harm" set forth in Article 3(20)[3] is extremely broad and, as explained in our comments in the breach notification section, does not provide a meaningful basis on which to trigger breach notification obligations under Article 25.

[3]"Harm" includes— (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (iii) financial loss or loss of property, (iv) loss of reputation, or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal."

***Significant harm.*** The definition of "significant harm" set forth in Article 3(38)[4], as discussed in the breach notification section, provides no practical way of measuring the degree of harm and does not account for the potential risk of harm.

***Significant Data Fiduciary.*** We recommend that entities that are already subject to an existing regulatory framework, such as those regulated under the Payment and Settlement Systems Act, not be included in this definition to eliminate the risk of overlapping or conflicting obligations.

***Critical Data.*** Critical Data should be limited to government data, which, if disclosed, would harm national security, sovereignty, friendly relations with foreign states, or legitimate public interest.

**4. Data Breach Notification (Article 25)**

***Notification Trigger.*** The definition of harm set forth in Article 3(20) establishes a very low threshold for triggering notification obligations under Article 25, one that is likely to result in over-notifying and desensitizing individuals to these important notices and inundating and overwhelming the Data Protection Authority. The goal of breach notification provisions should be to define a reasonable and balanced notification trigger that ensures that individuals receive notice when there is a significant risk of substantial harm as a result of a security breach but that does not result in over-notification.

The primary purpose of notification is to enable individuals to mitigate the risk of identity theft or fraud when a breach occurs. In contrast, the primary purpose of government reporting is to enable the Authority to exercise its regulatory oversight functions, for example, to identify persistent or systemic security problems and take action as needed to address those problems and to assist individuals who may be harmed by a breach. In addition, individual and government reporting obligations can serve to motivate organizations to implement more effective security measures to protect sensitive information. Setting the threshold too low, by including every "harm" possible rather than focusing on the more serious harms will undermine the goal of breach notification.

*Government.* Frequent reporting about relatively minor security breaches will overwhelm and deplete the resources of the Authority. Consequently, only major breaches (*e.g.*, those affecting more than 10,000 individuals) or breaches involving significant risk to individuals should be reported. A threshold should be selected that is most appropriate for a country's market size or in relation to the size of the organization.

*Individuals.* Any individual notification requirement should be risk based. In this regard, notification should focus on two types of risk and should be limited to situations where there

[4] Article 3(38) defines "Significant harm" as "harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm".

is a "significant risk" that sensitive information compromised in a breach will result in "significant harm," such as, for example, loss of business or employment opportunities because of an individual's health or a real risk of identity theft. Although serious, many, if not most, security breaches do not result in significant harm to the individuals to whom the breached information relates. For example, in many cases, media containing data about individuals is simply lost or misdirected without involving any misuse of the data. Any notification requirement should recognize that the risks associated with each breach will differ and, as a result, the appropriate response to each breach also will differ.

Similarly if a known third party inadvertently receives information that was misdirected and informs the company and deletes or returns the information, there is no risk of harm and notification will simply alarm individuals unnecessarily.

Moreover, notification in the wake of each incident of data breach, without regard to the high risk of substantial harm that might result, promises to have a counterproductive effect of overwhelming individuals with notices that bear no relation to the actual risks and, therefore, might not only needlessly frighten and confuse people, but also likely desensitize them and cause them to ignore the very notices that explain the action they need to take to protect themselves from harm when there is a significant risk.

**Definition of Specified Personal Information.** When imposing notification obligations, the law should specify the sensitive information that would be subject to these obligations. Specifically, notification should be based on the types of information that could be used to cause the harm that the notification requirement is designed to help individuals mitigate. With respect to a risk of identity theft or financial fraud, the notification obligation should be limited to identifiable and unencrypted data that includes one or more sensitive data elements, such as a national identification number (or other number that can be used to open a financial account) or financial account information together with any password or pin number that can be used to access the underlying account. With respect to a risk of substantial harm from the misuse of health information, the notification obligation should be limited to identifiable and unencrypted data that include an individual's name together with one or more sensitive health data elements, such as a social security number or government identification number or health information, such as, for example, a medical diagnosis ("Specified Personal Information").

In doing so, organizations can both work proactively to strengthen safeguards for this Specified Personal Information and, if various security breach incidents do occur, focus their responses on those incidents that relate to this information. Data that have been de-identified, encrypted or otherwise adequately secured (using other technology), however, should not be covered because an incident affecting such data does not pose a high risk of significant harm to individuals. Moreover, if the breach involves data that are publicly available, such data elements should be excluded from the risk analysis.

**Definition of a Data Breach.** In light of the discussion above, it would be preferable to define the types of data breaches that would trigger the need for notification. That definition

would specify the types of information that, if subject to a loss or unauthorized access or acquisition, are likely to result in "substantial harm" to the affected individuals. Focusing on specific types of data elements and the potential for substantial harm will yield more meaningful and helpful notifications. A determination of whether a particular incident poses a risk of substantial harm to the individual should be based on an assessment of the circumstances surrounding the particular incident. Simply applying the current definition of "harm" or "significant harm" is insufficient because it provides no practical way of measuring the degree of harm and does not account for the potential risk of harm.

**Notice Content.** Article 25(2)(c) requires data fiduciaries to specify the possible consequences of the breach. Specifying all of the possible consequences would be impossible and not very helpful. Instead, it would be better to require the fiduciaries to specify specific steps that individuals should take to protect themselves in the aftermath of the particular breach.

**Timing of Notification.** Article 25(3) requires data fiduciaries to report breaches to the Authority "as soon as possible and within such period as maybe specified by regulations, following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm". This provision should be modified to cover the carrying out of a reasonable internal and external (law enforcement) investigations as well as the adoption of any urgent remedy measures. Moreover, we caution the Authority about setting a specific time period such as 72 hours for Authority notifications and consumer notification. Establishing a short time period is unrealistic and will result in the notification containing insufficient information that will not be helpful either to regulators or individuals. That is now the situation in Europe where regulators are being overwhelmed by reports that are not fully fleshed out. It is better to receive good information rather than poor information after only 72 hours.

*Individuals*. While notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the scope and nature of the breach, remedying any ongoing breach and identifying the potentially affected individuals, the law should permit notification to be delayed at the request of a law enforcement agency in order to carry out its own investigation. For example, before notification is provided and before a breach is publicized in the media, law enforcement will have a better opportunity to catch the culprits involved (thereby, preventing future breaches from occurring or mitigating the harm felt by individuals).

The law should be flexible with respect to the method of notification. The most important feature should be to get notice to affected individuals in a timely way. The method used should depend on the particular circumstances surrounding the organization's relationship, if any, to the potentially affected individuals, the manner in which the organization typically communicates with them and the type and scope of the breach. For example, some organizations, such as banks, regularly mail monthly statements to account holders. Consequently, postal mail notification may be the most logical choice for these

organizations. Alternatively, other organizations may rely more on their websites as their means to communicate with their customers and potential customers and, therefore, should be permitted to use electronic methods to notify individuals. In addition, website notification or other methods of mass communication may be more appropriate when a breach involves large numbers of individuals (*e.g.*, 1,000-250,000 individuals) or if the organization does not have proper contact information.

Consequently, organizations should be permitted to select the most appropriate and effective method of communication, taking into account the way in which the organization typically communicates with individuals and the circumstances surrounding a given breach. Acceptable methods of communication should, therefore, include direct notice by postal mail, e-mail, telephone, or face-to-face communications, or through generally accessible notification methods (*e.g.*, website information, posted notices or mass media). Mass communications may be appropriate if direct notification is likely to cause further harm, is prohibitive in cost or the contact information for potentially affected individuals is not known. Moreover, using multiple methods of notification in the same security incident depending on the relationship with the individual in certain cases may also be appropriate.

While the Act currently allows the DPA to make decisions on how and whether to notify the impacted individuals, the DPA should not be the final arbiter. Data fiduciaries should make these decisions (potentially with input from the DPA). This will also allow data fiduciaries to provide consistent information if an incident has global effects.

Finally, we recommend clarifying that the DPA cannot publish information about the incident on its website before a data fiduciary provides notification to individuals. Often the short time frames required to notify regulators will not give data fiduciaries time to investigate an incident and be ready to make public statements. The ability of a DPA to publish information too early could drive data fiduciaries to make public statements about incidents more quickly than they normally would in a breach investigation and this could lead to unnecessary concern to data principals if upon further investigation, no impact was discovered. It may also have a chilling effect on the timely reporting of such incidents.

**5. Penalties**

We believe that the penalties proposed under the Act are excessive and may restrict economic activity and growth. We recommend that criminal penalties be eliminated from the Act because they are likely to have a chilling and deterrent effect on business entry into the Indian marketplace. Imposition of civil penalties can provide sufficient incentives to encourage compliance. Such civil penalties, however, should be reasonable otherwise they too will discourage marketplace entry. Basing penalties on total worldwide turnover is excessive and has the potential to bankrupt companies for a single global incident. It will also create a disincentive for the company to work proactively with regulators to address any

problems that may emerge. In addition, such high penalties will inevitably lead to litigation and will prolong any resolution of investigations and the payment of the penalties. A more appropriate and fair approach would be to base penalties on the amount of turnover within India, an approach that would correspond with the actual activities of the company in India.

## ADDITONAL RECOMMENDATIONS

### 1. Data Protection Impact Assessment (Article 27)

***When a DPIA is required.*** Article 27(1), read in conjunction with Article 28, requires significant data fiduciaries to carry out data impact assessments prior to undertaking any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to individuals. In addition, Article 27(2) empowers the Authority to specify additional circumstances or classes of data fiduciaries or processing operations where data protection impact assessments (DPIAs) will be required.

DPIAs are valuable tools that can be used by organizations to identify and mitigate risks that certain new technologies, operations or measures pose a high risk to privacy. The use of DPIAs by data fiduciaries should certainly be encouraged but should not be mandated unless there is a serious risk of negative and unknown consequences to privacy. For example, it does not make sense to mandate DPIAs when the consequences are already known and certain measures and procedures are commonly applied or before every new technology or procedure is introduced. In addition, the frequency of such impact assessments should be determined by the organization itself so that it does not become another costly and unnecessary administrative burden.

Therefore, we urge the government to limit the DPIA requirement to processing that poses a "serious risk of negative and unknown consequences to privacy". This approach is similar to the GDPR's DPIA approach which requires that DPIAs be undertaken when the envisioned processing is likely to result in a "high risk to the rights and freedoms of natural persons". Imposing a lower standard – one that triggers DPIAs for processing that is not high risk -- is overly burdensome, costly and unnecessary.

***Public disclosure of DPIAs.*** The requirement under Article 27(4) to submit DPIAs to the Authority should be limited to situations where the data fiduciary is unable to mitigate the risks from such processing. This is the approach used under the GDPR. In addition, any DPIAs submitted to the Authority should not be made public. To do otherwise will discourage their use and possibly compromise the integrity of the assessment itself and the overall security of the product or service. Their value as a powerful internal tool enabling organizations to manage and mitigate their risks would be severely undermined.

Organizations that do carry out such assessments should maintain appropriate records that can be inspected by authorities in the event of a compliance or enforcement investigation.

**2. Data Protection Officer (Article 30)**

Article 30(1)(g) requires the Data Protection Officer (DPO) to maintain an inventory of all of the records required under the data protection law. While the DPO should be able to comment on or assist in the development and maintenance of these records, the data fiduciary should be given greater flexibility to assign that responsibility, based on its particular organizational structure. It may be more efficient for the company to assign that responsibility to another person or department within the organization.

Article 30(3) requires that significant data fiduciaries not present in India that carry on processing covered by the law to appoint an India-based DPO. We urge the government to consider a more flexible approach – one that would enable the data fiduciary to select its DPO based on qualifications and organizational structure rather than physical location. For example, under the GDPR, one DPO can be designated for a group of undertakings, provided that the DPO is "easily accessible from each establishment". This means that individuals, the relevant DPAs, and the employees within each covered organization must be able to reach the DPO easily, directly, and confidentially without having to contact another part of the organization. The Working Party 29 acknowledges that where the organization has no establishment within the EU, a DPO may be able to carry out his/her activities more effectively if located outside the EU.

Moreover, the EU allows the DPO function to be outsourced to an individual or an organization. It recognizes that it is possible that individual skills and strengths are combined so that several individuals, working in a team, perform the DPO function.

**3. Complaint Handling (Article 32)**

Article 32(3) requires data fiduciaries to resolve complaints within thirty days from the date of receipt of grievance. It is unrealistic and unreasonable to expect that organizations will be able to resolve the complaints within such a short period. Complaints often take time to resolve; some may be more complicated than others. Instead, it would be more reasonable to require organizations to respond to complaints within 30 days without mandating a specific timeframe for resolution of any grievances.

4. **Access Requests (Article 17)**

The Act heightens a data fiduciary's disclosure obligations as part of an access request by granting individuals "the right to access in one place the identities of the data fiduciaries with whom his personal data have been shared by any data fiduciary together with the categories

of personal data shared with them." However, this language is very broad. Data may be shared with a third party for legitimate business purposes where the data are not the focus of the transaction. We recommend that the language be narrowed to focus on those situations that are addressed in other recent data protection laws, such as when personal data are sold to a third-party data broker. We recommend the following language: "the right to access in one place the identity of the data fiduciaries with whom his personal data have been sold or transferred for monetary consideration."

**5. Power of Central Government to exempt certain data processors. (Article 37)**

The scope of this provision should cover the processing of *all* personal data, *including sensitive personal data* of individuals not within the territory of India, because such processing is already regulated under other local data protection regulations.