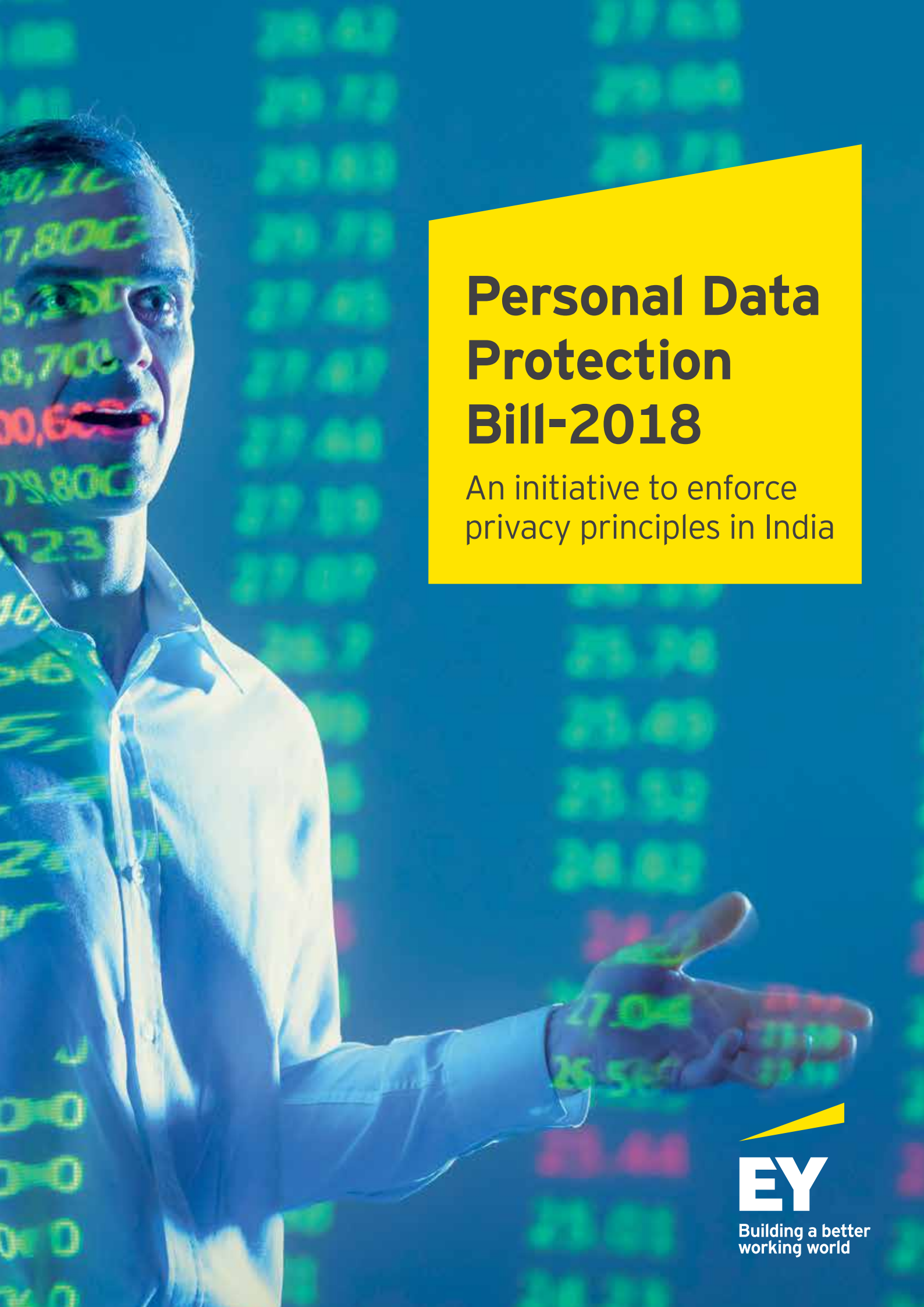


Personal Data Protection Bill-2018

An initiative to enforce privacy principles in India

EY
Building a better working world

Introduction

In year 2017, the Government of India constituted a committee of experts under the chairmanship of former Supreme Court Justice Shri B N Srikrishna to study various issues relating to data protection in India and make specific suggestions on principles to be considered for data protection in India and suggest a draft Data Protection Bill. The committee, formed with the idea to create a powerful data protection law in India, has submitted its draft bill to the Ministry of Electronics and Information Technology (MeitY) on 27 July 2018. This submission comes after a year of consultations with various stakeholders.

The bill lays down penalties, ranging from five crore rupees or 2% of total global turnover to fifteen crore rupees or 4% of the total global turnover*. It is thus changing the way privacy is perceived and practiced within Indian business.

Who is subject to the data protection bill?

The proposed bill applies to both government and private entities. The applicability of the law will extend to data controllers/fiduciaries or data processors not present within the territory of India, if they carry out processing of personal data in connection with:

- Any business carried in India
- Systematic offering of good and services to data principles (also generally referred to as data subject) in India
- Any activity which involves profiling of data principals within the territory of India

This document highlights the key requirements of the data protection bill and further encapsulates the key steps that the Indian organizations should undertake that handle personal data.

Data Protection Bill at a glance

What is the Data Protection Bill?

The objective of the bill is to ensure a free and fair digital Indian economy and it is seen as an critical step in setting up a privacy framework which gives the Indians full freedom to protect their personal data.

Who will be impacted by the bill?

It applies to private and government sectors.

- It applies to any business carried in India
- Goods and services offered to data principals in India
- Any activity involving profiling of Indians

The definition of **personal data** is defined on the parameters of identifiability.

characteristics	Traits	Attributes
		

The new data protection bill

Is an important pillar in the Indian privacy ecosystem

Data subjects have the **right to be forgotten** and erased from records

Users may request a copy of personal data in a **portable format**

Users have right to **correction** and right to **confirmation**

Tough penalties

Fines up to

2%-4%	or	INR 5-15 crore
of total worldwide turnover		whichever is greater

All personal data, sensitive personal data and children data stored should be obtained by **consent**

Sensitive/critical personal data should be stored in India only.

For any processing activity of personal data inside or outside India, one **"mirror copy"** shall be required to be retained in India.

Data Fiduciary shall take steps to maintain **transparency** regarding general practices relating to **processing of personal data** . Follow principles of **record keeping, data audits, Data Protection Impact Assessment**

Appoint a **data protection officer** as per their processing activities

Products, systems and processes must consider **privacy-by-design** concepts during development

Key highlights for a data fiduciary*

- **Grounds for processing personal data** include consent, functions of state, compliance with law or order of court/ tribunal, for prompt action in case of emergencies, purposes related to employment or reasonable purposes of the data fiduciary
- **Grounds for processing sensitive personal data** include explicit consent, functions of state, compliance with law or order of court/tribunal, for prompt action in case of emergencies for passwords, health data, financial data, official identifiers, genetic data and biometric data
- Age verification and parental consent is required for processing personal and sensitive **personal information of children**
- **Transparency and accountability** principles such as privacy by design, record keeping, data protection impact assessment and data audits should be undertaken by organizations
- Organizations will have to appoint a **data protection officer** as per their processing activities
- **Data breaches** have to be reported by data fiduciaries to the authority and based on the gravity of the incident the same has to be notified to the data principal
- Adequate **security controls** should be in place: de-identification, encryption, prevention of unauthorized access, misuse, disclosure or destruction
- Restrictions have been imposed on **transfer of personal data outside India** for sensitive critical personal data. For other personal data one local copy (mirroring provisions) has to be maintained in India only
- Organizations will have to build capability to complete **data principal rights**

- **Personal data:** Means data about or relating to a natural person who is directly or in-directly identifiable, having regard to any characteristic, trait, attribute, or any other feature of identity of such natural person or any combination of such features, or any combination of such features with other information
- **Sensitive personal data:** Means personal data revealing, related to, or constituting, as maybe applicable, passwords, financial data, heath data, official identifier, sex data, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste/tribe, religious or political belief or affiliation or any other category of data specified by authority under section 22

*Source-https://www.dsci.in/sites/default/files/Personal-Data-Protection-Bill-2018-Highlights.pdf

Emergence of Data Protection Bill

2017 — On 31 July 2017, the Ministry of Electronics & Information Technology set up the Justice BN Srikrishna Committee to draft a data protection law

2017 — On 27 November 2017, the committee released a white paper to give seven key principles to data protection, seeking public comments

2018 — Four rounds of public consultation meetings were held in the month of January 2018 inviting stakeholders to give their suggestions on the draft data protection framework

2018 — On 27 July, 2018 MeitY released Justice BN Srikrishna Committee Experts' report on Data Protection as well as the first draft of Personal Data Protection Bill, 2018

Key highlights for data principals/data subjects

- When an individual no longer wants their data to be processed, the data must be deleted **("right to be forgotten")**
- Individuals have the right to more information on how their data is processed, available in a clear and understandable way **("right to confirmation and access")**
- Data principals can get their personal information updated, corrected and completed **("right to correction")**
- Data principals can port their data making it easier for individuals to transmit personal data between service providers **("right to portability")**
- An individual has the right to know when their **data has been breached**

Preparing for the future:
What should organizations do?

Accountability of data protection

Data fiduciaries need to maintain accountability for the personal data they own and assert the responsibility to comply with the personal Data Protection Bill. Organizations need to be transparent and fair in terms of

Key considerations

- **Privacy governance:** Establish a personal data governance framework defining roles and responsibilities of key stakeholders of the privacy and compliance team
- **Provide a fair and transparent notice** to the data principals while collecting their data describing the collection, use, access, storage, disclosure, security of the personal data along with the choice and their rights. This should be applied for both online and offline collection modes
- **Update the digital presence:** Organizations need to review their digital presence in line with the requirements of the bill- update their privacy statements, cookie policy, consent mechanism and online terms and conditions. Also, solutions will have to be implemented for management of cookies
- **Refresh consents:** Organizations need to ensure that personal data is processed after obtaining valid consents from data principals. Explicit consent should be obtained for processing sensitive personal data. Pre-ticked boxes are no longer accepted as a valid consent. Organizations may explore automated solutions for managing and storing consents
- **Consent for children:** Personal data of children should be processed after verifying the age of the children and obtaining parental consent. Any organization processing the personal data of children may need to include age as a compulsory parameter and use it further to identify minor cases
- **Review data processing activities:** Review the data currently being collected for data principals and ensure that only the minimum personal data fields are collected from the users, which are critical to fulfil the purpose of processing the data and provide the product/ service requested by the data principal
- **Accuracy:** Steps need to be undertaken to ensure that data collected is complete, accurate and correct

Data localization and mirroring

Data fiduciaries will need to store at least a copy of the personal data acquired by data principals in India. Additionally, the central government may describe categories of "critical data" which has to be stored only in India. This would require organizations to perform an assessment their data storage practices and maintain servers/ data centres in India, if needed, to fulfil the obligation. Contractual agreements approved by the authority need to be in place for transferring personal data outside India.

Key considerations

- **Review the current data storage practices** in the organization and identify all the locations where personal data is stored including cloud storage
- **Formulate strategies** for maintaining a copy of personal data in a server/ data center in India. Also, reconsider current storage solutions with alternative solutions to ensure that maintenance of redundant copies may not become cumbersome for the organizations
- **Restrict transfer of critical data*:** Based on the definition given by the government of India (to be released) identify "critical data" and refrain from storing it outside Indian territory, unless exempted by the authority and the central government*
- **Review cross border data transfers:** Global organizations serving Indian customers will have to relook at their cross border movement practices and plan the locations/data centers in which data will be stored within India

Privacy by design and default

The draft bill proposes that data fiduciaries be obligated to take necessary measures and implement policies to ensure that privacy is embedded in all the systems, applications and architecture at each stage- collection, processing, usage, transmission, storage and disposal. Additionally, it requires data fiduciaries to implement appropriate safeguards to ensure security of the personal data.

Key considerations

- **Current state technical privacy assessment:** Assess the current security and privacy posture of the existing IT systems, applications and architectures that capture personal data and establish appropriate security controls depending on the existing environment to avoid unauthorized access, disclosure, alteration or destruction of personal data
- **Introduce safeguards** such as encryption, pseudonymisation at each stage of the personal data lifecycle, from ingress to egress of personal data in the environment of the organization
- **Identify compensating controls** for legacy systems with technical limitations
- **Embedding privacy in design:** For new systems and processes introduce a privacy by design program to ensure that the systems are not live before obtaining the privacy clearance
- **End to end security:** Introduce measures to ensure confidentiality, integrity and availability of data

Data principal rights

The personal data protection bill intends to confer controlling power in the hands of the data principles and hence provides them with the right to access and correction, the right to data portability and right to be forgotten. It attempts to provide its citizens with comprehensive data protection rights and create a trust based relationship between the data principal and the data fiduciary.

Key considerations

- **Communication to data principals:** Communicate the rights of the data principals at the time of data collection and how they can exercise those rights (channels through which the request can be received)
- **Data principal management procedure:** Establish and implement a process to manage and respond to requests for exercising the rights, which includes validating, logging and acknowledging the request followed by fulfilling and responding to the data principal. Also, the timelines for completion of the request have to be determined by the organization. Exception cases wherein the request cannot be fulfilled have to be chalked out
- **Data mapping:** Organizations will have to map the end to end personal data flows (collection, processing, transfer, disclosure, storage and disposal) so that the data principal requests can be fulfilled within the given timelines

Data breach management

The draft bill requires data fiduciaries to inform the data protection authority any personal data breach that is likely to cause harm to any data principal. Failure to notify a breach will make the organization liable to a penalty under the provisions of this bill.

Unlike other global privacy regulations, the Data Protection Bill does not specify the exact timelines within which data breaches should be reported

Key considerations

- Identify and discover all personal data the organization holds, the vulnerabilities, possible threats and leakage points such as third party access, external sharing, network vulnerabilities, corporate espionage, etc. and design a comprehensive incident response plan
- Establish/update existing incident management procedures to include an end to end workflow for management of a personal data breach. Incorporate personal data breach notification mechanism in the existing incident management tool. The procedure should highlight the need to conduct a root cause analysis of all incidents
- Categorize incidents: Identify and define what a personal data breach could be and categorize them basis the severity (based on data type, number of data principals, etc.) and the likelihood of causing a harm to the data principal
- Reporting to DPA: Establish mechanisms to identify a data breach and design a process for reporting the incident of a possible data breach to the authority. Based on the severity, notify data principals as well through channels such as posting details on the website. Communication templates should be designed for notifying the data principals and DPA. Also, clauses should be included in the third party contracts related to notification of a breach from the vendors end

Data storage limitations

Data fiduciaries need to identify the retention periods for personal data and conduct regular reviews to ascertain the need to retain the personal data.

Key considerations

- **Draft data retention policy** organizations will have to draft retention policies highlighting the retention schedules (such as short term, standard and prolonged storage) for each data type collected and processed for data principals. The retention period needs to be drafted considering the legal, regulatory and business requirements. Policy should also be drafted for the backup and archived data
- **Secure disposal:** When the data is no longer required as per the policy, organizations should develop a secure disposal policy. Solutions/ tools should be used to discard the data securely
- **Anonymization:** For critical data types that need to be stored for prolonged periods or beyond the retention period, organizations may consider solutions such as anonymization to ensure security of personal data
- **Conduct reviews:** Procedures to conduct regular review of the retention schedule should be in place to ensure that data is retained as per the retention policy only and additional unwanted data is disposed securely

Enhance security of personal data

Every data fiduciary and data processor shall undertake a review of its security safeguards periodically and take appropriate measures accordingly to ensure security of personal data

Key considerations

- Relook at existing security controls organizations should assess the existing security controls and solutions to meet the privacy requirements of the bill. Also, the same should be enforced on the partners and vendors processing personal data on behalf of the data fiduciary
- Implementation of technical and organizational solutions including effective monitoring and auditing of changes to databases, data loss prevention solutions, malicious attacks or data handling misuse, secure audit trails, monitoring access to personal data through identity and access management, thus, providing a higher level of access control for sensitive data. Implement encryption, de-identification tools
- Training and awareness: The draft bill proposes a plethora of changes, which would require organizations to largely reconsider their personal data handling practices. Organizations need to introduce the principle of data privacy in the core of all their processes. This paradigm shift requires organizations to extensively train their personnel regarding data privacy and safe data handling practices

Additional ask for significant data fiduciary

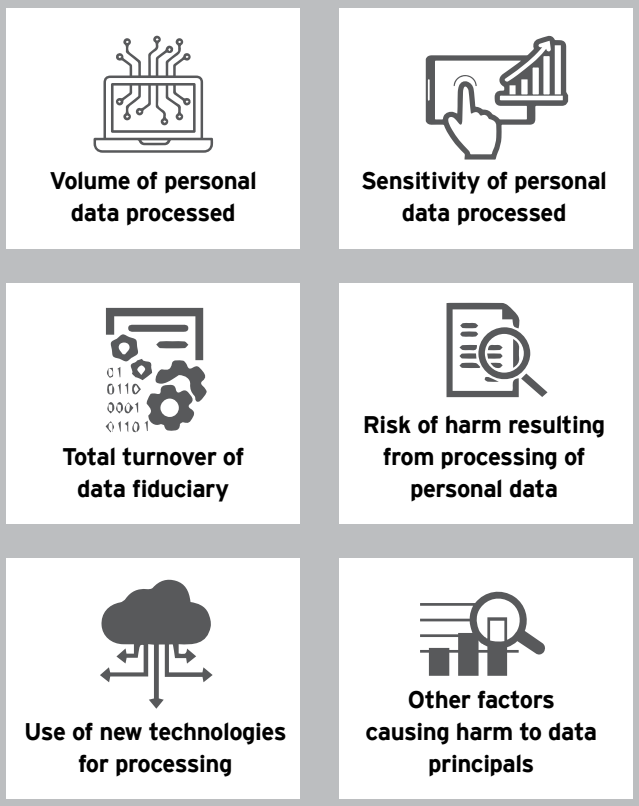
The Draft Bill lays down certain additional obligations that apply to a specific class of data fiduciaries conducting high risk processing known as Significant Data Fiduciary.

To identify if an organization qualifies to be categorized as a Significant Data Fiduciary, the authority would consider the parameters given in the adjacent figure.

Key considerations

- Identify if the organization comes under the category of Significant Data Fiduciary according to the parameters defined by the data protection bill
  - If yes, consider the following:
  - Register with the data protection authority
  - Undertake data protection impact assessments (DPIA) for high risk processing
  - Appoint a data protection officer
  - Get the privacy policies and the conduct of processing of personal data audited annually by an independent data auditor

Figure: Factors for consideration of significant data fiduciary



*Source:http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdfs

How can EY help?

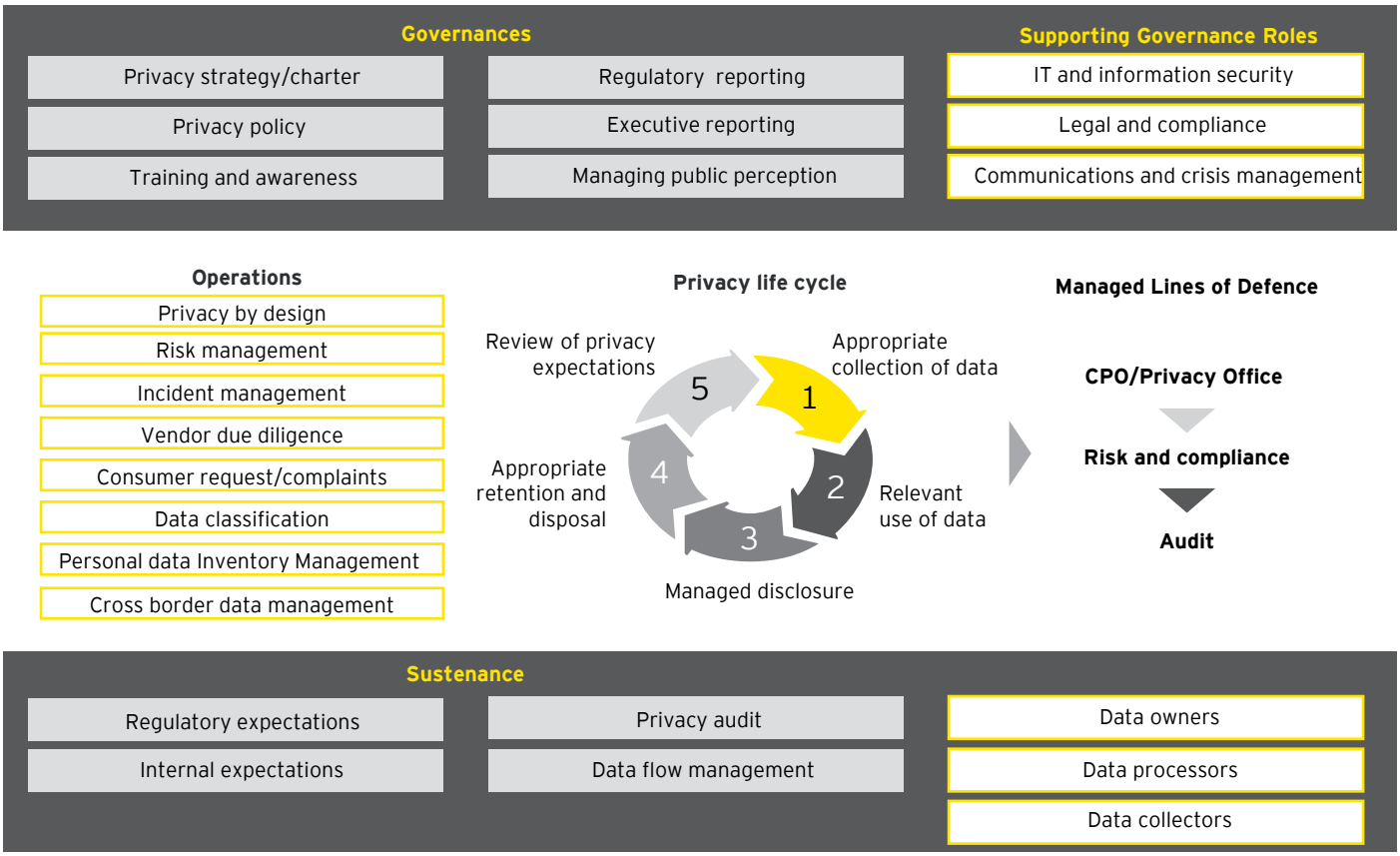
EY has a team of over 200 Certified Information Privacy Professionals (CIPPs) and privacy lawyers who help organizations to better understand what risks exist with respect data privacy and compliance with the upcoming personal data protection regulation of India.

For over a decade, EY has assisted international organizations in understanding privacy and data protection risks, compliance as well as regulations, thereby helping them effectively manage the use of personal data within their organizations.

We can help you deliver and run privacy improvement programs by leveraging our senior stakeholder management expertise, privacy framework, mature tools, methodologies and flexible resourcing models.

Our privacy portfolio

- Privacy transformation program
- Current state assessment
- Data protection impact assessment
- Personal information and inventory data flow
- Vendor risk management



For questions about privacy and cybersecurity, please contact

Nitin Bhatt
Global Leader-Risk Transformation
Email: nitin.bhatt@in.ey.com

Burgess Cooper
Partner-Cyber Security, EY
Email: Burgess.cooper@in.ey.com

Kartik Shinde
Partner-Cyber Security, EY
Email: kartik.shinde@in.ey.com

Tiffy Issac
Partner-Risk Advisory, EY
Email: Tiffy.issac@in.ey.com

Rahul Naik
Partner-Cyber Security, EY
Email: Rahul.naik@in.ey.com

Prashant Choudhary
Partner-Cyber Security, EY
Email: prashant.choudhary@in.ey.com

Vidur Gupta
Partner-Cyber Security, EY
Email: vidur.Gupta@in.ey.com

Jaspreet Singh
Partner-Cyber Security, EY
Email: Jaspreet.singh@in.ey.com

Mini Gupta
Partner-Cyber Security, EY
Email: mini.gupta@in.ey.com

Notes

EY offices

Ahmedabad
2nd floor, Shivalik Ishaan
Near. C.N Vidhyalaya Ambawadi
Ahmedabad-380015
Tel: +91 79 6608 3800
Fax: +91 79 6608 3900

Bengaluru
12th & 13th floor
"U B City" Canberra Block
No.24, Vittal Mallya Road
Bengaluru-560 001
Tel: +91 80 4027 5000
+91 80 6727 5000
Fax: +91 80 2210 6000 (12th floor)
Fax: +91 80 2224 0695 (13th floor)

1st Floor, Prestige Emerald
No.4, Madras Bank Road
Lavelle Road Junction
Bengaluru-560 001 India
Tel: +91 80 6727 5000
Fax: +91 80 2222 4112

Chandigarh
1st Floor SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh-160 009
Tel: +91 172 671 7800
Fax: +91 172 671 7888

Chennai
Tidel Park 6th & 7th Floor
A Block (Module 601,701-702)
No.4, Rajiv Gandhi Salai Taramani
Chennai-600113
Tel: +91 44 6654 8100
Fax: +91 44 2254 0120

Delhi NCR
Golf View Corporate Tower – B
Sector 42, Sector Road
Gurgaon–122 002
Tel: +91 124 464 4000
Fax: +91 124 464 4050

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity New Delhi-110037, India
Tel: +91 11 6671 8000
Fax +91 11 6671 9999

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
NOIDA-201 304
Gautam Budh Nagar, U.P. India
Tel: +91 120 671 7000
Fax: +91 120 671 7171

Hyderabad
Oval Office
18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500081
Tel: +91 40 6736 2000
Fax: +91 40 6736 2200

Jamshedpur
1st Floor, Shantiniketan Building,
Holding No. 1, SB Shop Area,
Bistupur, Jamshedpur – 831001
Tel: 657 663 1000

Kochi
9th Floor "ABAD Nucleus"
NH-49, Maradu PO
Kochi - 682 304
Tel: +91 484 304 4000
Fax: +91 484 270 5393

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400
Fax: + 91 33 6615 3750

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (west)
Mumbai-400 028, India
Tel: +91 22 6192 0000
Fax: +91 22 6192 1000

5th Floor Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai-400 063, India
Tel: +91 22 6192 0000
Fax: +91 22 6192 3000

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000
Fax: + 91 20 6601 5900

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN1808-007
ED None

JS

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or, more specifically, on achieving growth or optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/advisory

ey.com/in

@EY_India EY|LinkedIn EY India EY India careers ey_indiacareers