Digital Personal Data Protection Act (DPDPA) 2023

A Deep dive into Legal obligations and implementation readiness

23 SEPTEMBER 2023

ISACA®
Chennai Chapter

Speakers

Sakthi Thangavelu CIPM

Independent Consultant,
Founder, www.ethically.in

Privacy regulatory
compliance

Sakthi@ethically.in

Raja Krishnan CIPP/E

Lead – Legal vertical,
Corporate Law and Secretarial
Practitioner

Akshyam Corporate Advisors, Chennai

raja.krishnan@akshayamcorporate.com

ISACA®
Chennai Chapter

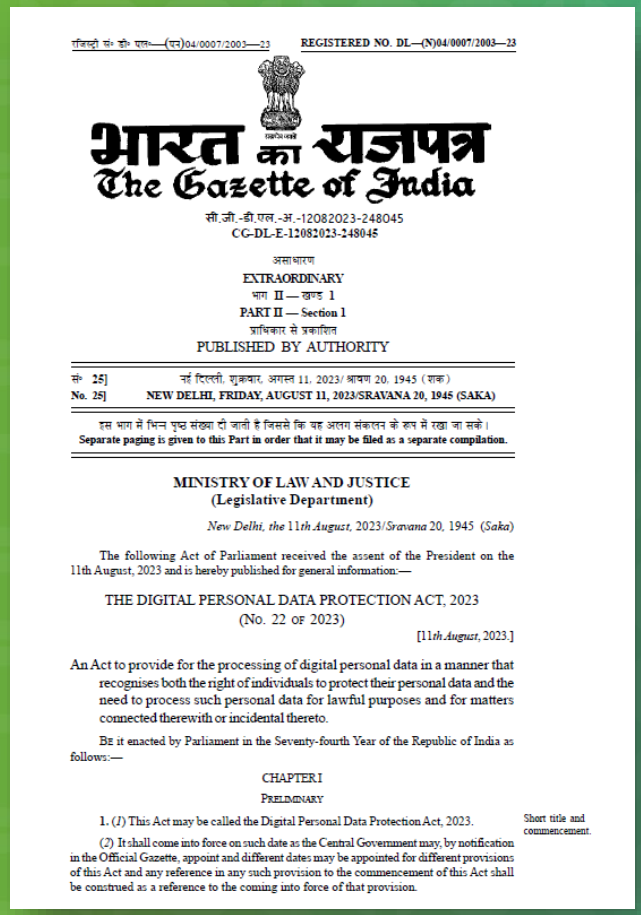
Agenda

1. DPDPA 2023 – the journey so far

2. Level setting – Key stakeholders in DPDPA

3. The legal construct
    1. Definitions
    2. Legal obligations for enterprises
    3. Implementing the obligations by enterprises
    4. Legal obligations for Individuals
    5. Data Protection Board - The regulatory body
    6. Processing outside India and Exceptions
    7. Penalties

4. Readiness / Next steps



रजिस्ट्री सं० डी० एल०—(एन)04/0007/2003—23 REGISTERED NO. DL—(N)04/0007/2003—23

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-12082023-248045
CG-DL-E-12082023-248045

असाधारण
EXTRAORDINARY
भाग II — खण्ड 1
PART II — Section 1
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं० 25] नई दिल्ली, शुक्रवार, अगस्त 11, 2023/ श्रावण 20, 1945 (शक)
No. 25] NEW DELHI, FRIDAY, AUGUST 11, 2023/SRAVANA 20, 1945 (SAKA)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।
Separate paging is given to this Part in order that it may be filed as a separate compilation.

MINISTRY OF LAW AND JUSTICE
(Legislative Department)

New Delhi, the 11*th August*, 2023/*Sravana* 20, 1945 (*Saka*)

The following Act of Parliament received the assent of the President on the 11th August, 2023 and is hereby published for general information:—

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
(No. 22 OF 2023)

[11*th August*, 2023.]

An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Seventy-fourth Year of the Republic of India as follows:—

CHAPTER I
PRELIMINARY

1. (*1*) This Act may be called the Digital Personal Data Protection Act, 2023. Short title and commencement.

(*2*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

ISACA®
Chennai Chapter

DPDPA 2023 – the journey so far

ISACA
Chennai Chapter

The Making Of The Digital Personal Data Protection Act, 2023

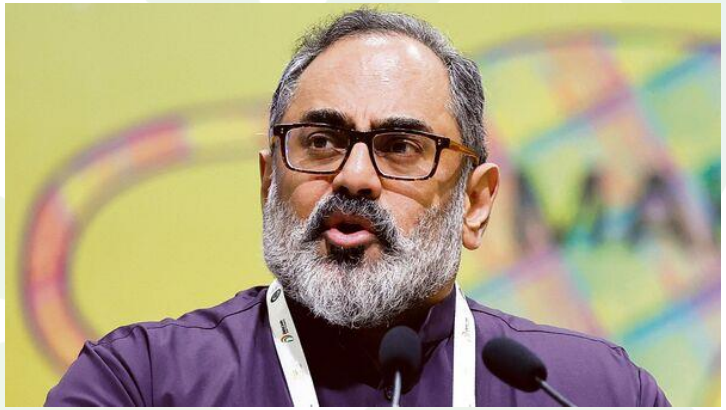
July 2017	• MeitY constitutes an expert committee under the chairmanship of Justice BN Srikrishna
August 2017	• Supreme Court, while hearing the Aadhaar-case in Justice KS Puttaswamy vs Indian Govt, recognises right to privacy as a fundamental right; orders govt to introduce relevant law • Justice Srikrishna Committee on data protection constituted
July 2018	• MeitY releases Justice Srikrishna Committee report and proposed draft Bill
December 2019	• Revised Personal Data Protection Bill introduced in Lok Sabha • The Bill referred to Joint Parliamentary Committee (JPC)
December 2021	• JPC submits its report along with a new draft Bill — PDP Bill 2021
August 2022	• The Indian Govt withdraws the draft PDP Bill 2021 from Lok Sabha
Nov 2022	• MeitY releases a fresh new draft called DPDP Bill, 2022 for public consultation
August 2023	• Govt introduces DPDP Bill 2023 in Lok Sabha • Parliament enacts the Bill

Source: Inc42

Inc42

Data Protection Board, relevant rules likely in a month

The first set of necessary rules under the Act will be issued within 30 days, said minister Rajeev Chandrasekhar



20th Sep 2023 New Delhi: The government will set up the data protection board (DPB), the appellate authority for grievance redressal under the Digital Personal Data Protection Act, within the next 30 days, Rajeev Chandrasekhar, minister of state for electronics and information technology said on Wednesday. The first set of 'necessary rules' under the Act will also be issued within the same time frame.

ISACA® Chennai Chapter

Key Stakeholders & terminologies - level setting

ISACA Chennai Chapter

Key Stakeholders called out in DPDPA 2023

Data Principal

The individual to whom the personal data relate

Data Fiduciary

- Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data
- A Data Fiduciary becomes “Significant” Data Fiduciary based on certain types of processing to be notified later.

Data Processor

Any person who processes personal data on behalf of a Data Fiduciary

Data Protection Officer

Individual appointed by Significant Data fiduciary; based in India; responsible to the governing body of the company; point of contact for grievance redressal

Consent Manager

- a person registered with the Board
- Who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent
- through an accessible, transparent and interoperable platform

Data Auditor

Who carry out data audit, who shall evaluate the compliance of the Significant Data Fiduciary in accordance with the provisions of this Act

A person

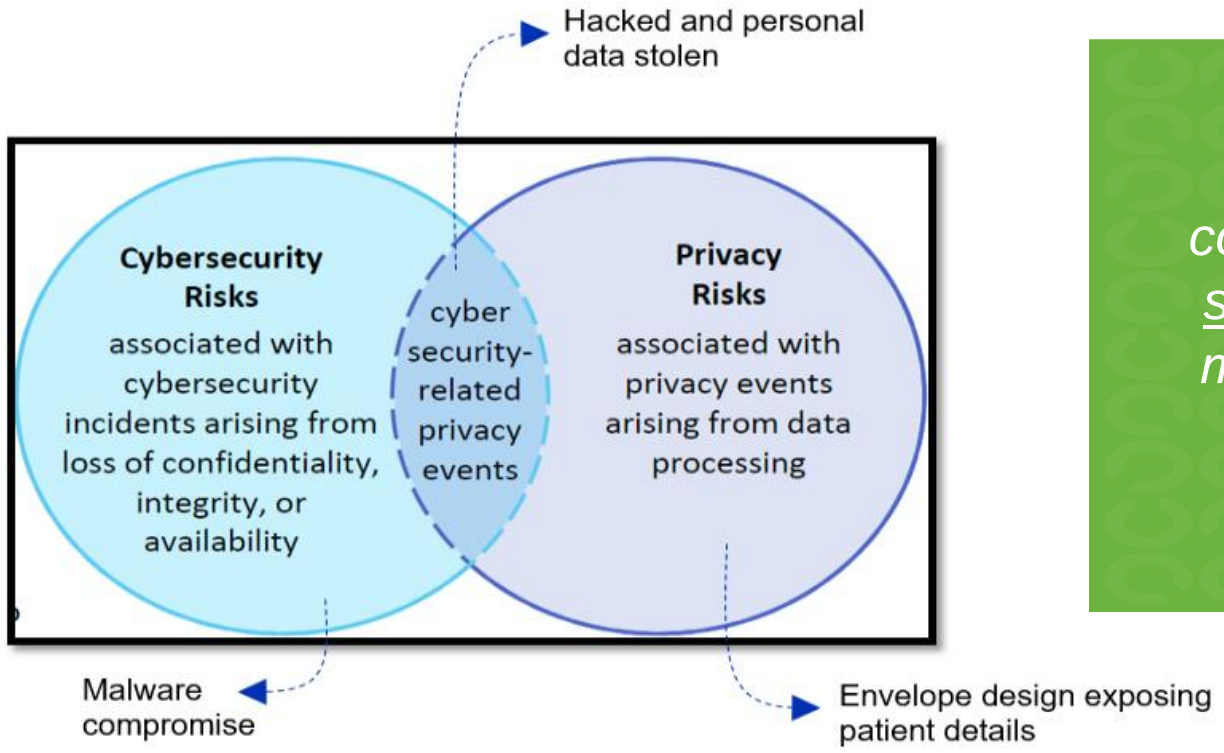
A person includes an Individual, a Hindu undivided family, a company, a firm, an association of persons, body of individuals, a State or an artificial juristic person not falling within the above

ISACA®
Chennai Chapter

Data Privacy, Data Protection

Data privacy is concerned with collection, proper handling, processing, storage and usage of personal information. Its about the rights of individuals with respect to their personal information.

Data protection is concerned with protecting personal data from any unauthorized access or malicious attacks and exploitation of data. It is set up to protect personal data using different methods and techniques to ensure data privacy.



"While managing cybersecurity risk contributes to managing privacy risk, it is not sufficient, as privacy risks can also arise by means unrelated to cybersecurity incidents"

NIST PRIVACY FRAMEWORK

ISACA Chennai Chapter

Dissecting the law
- the Legal construct

ISACA®
Chennai Chapter

DPDPA 2023 in a page

CHAPTER I: PRELIMINARY (Sections 1 to 3)

1. Short title and commencement
2. Definitions
3. Application of Act

CHAPTER II: OBLIGATIONS OF DATA FIDUCIARY (Sections 4 to 10)

4. Grounds of processing personal data
5. Notice
6. Consent
7. Certain legitimate uses
8. General obligations of Data Fiduciary
9. Processing of personal data of children
10. Additional obligations of Significant Data Fiduciary

CHAPTER III: RIGHTS AND DUTIES OF DATA PRINCIPAL (Sections 11 to 15)

11. Right to access information about personal data
12. Right to correction and erasure of personal data
13. Right of grievance redressal
14. Right to nominate
15. Duties of Data Principal

CHAPTER IV: SPECIAL PROVISIONS (Sections 16 and 17)

16. Processing of personal data outside India
17. Exemptions

CHAPTER V: Data Protection Board of India (Sections 18 and 26)

18. Establishment of Board
19. Composition and qualifications for appointment of Chairperson and Members
20. Salary, allowances payable to and terms of office
21. Disqualifications for appointment and continuation as Chairperson and Members of Board
22. Resignation by Members and filling of vacancy
23. Proceedings of Board
24. Officers and employees of Board
25. Members and officers to be public servants
26. Powers of Chairperson

CHAPTER VI: POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD (Sections 27 and 28)

27. Powers and functions of Board
28. Procedure to be followed by Board

CHAPTER VII: APPEAL AND ALTERNATE DISPUTE RESOLUTION (Sections 29 to 32)

29. Appeal to Appellate Tribunal
30. Orders passed by Appellate Tribunal to be executable as decree
31. Alternate dispute resolution
32. Voluntary undertaking

CHAPTER VIII: PENALTIES AND ADJUDICATION (Sections 33 and 34)

33. Penalties
34. Crediting sums realized by ways of penalties to Consolidated Fund of India

CHAPTER IX: MISCELLANEOUS (Sections 35 to 44)

35. Protection of action taken in good faith
36. Power to call for information
37. Power of Central Government to issue directions
38. Consistency with other laws
39. Bar of jurisdiction
40. Power to make rules
41. Laying of rules and certain notifications
42. Power to amend Schedule
43. Power to remove difficulties
44. Amendments to certain Acts

THE SCHEDULE – Breach types and Penalties

ISACA Chennai Chapter

DPDPA 2023

ISACA Chennai Chapter

Definitions

- Data Management
- Usage and Sharing
- Data Control

- Representation of fact, concepts
- in a manner suitable for communication / processing
- Human / automated means
- Agnostic to medium or format used to convey

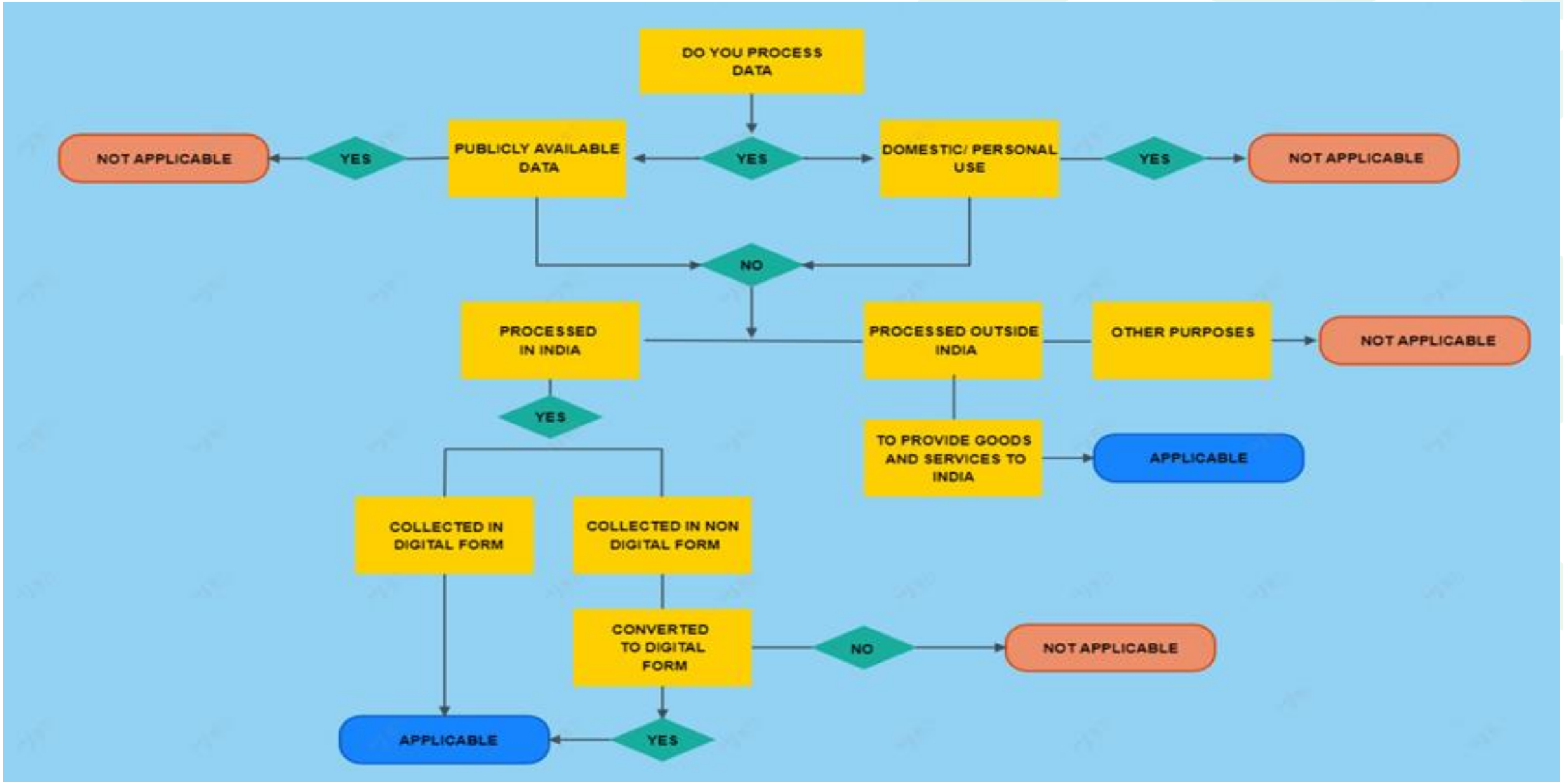
Processing of Digital Personal Data

Personal Data, in Digital form

- Data about individuals
- Identifiable by / in relation to such Data

ISACA Chennai Chapter

Determining the DPDPA Scope



DPDPA 2023

CHAPTER I: PRELIMINARY (Sections 1 to 3)

1. Short title and commencement
2. Definitions
3. Application of Act

CHAPTER II: OBLIGATIONS OF DATA FIDUCIARY (Sections 4 to 10)

4. Grounds of processing personal data
5. Notice
6. Consent
7. Certain legitimate uses
8. General obligations of Data Fiduciary
9. Processing of personal data of children
10. Additional obligations of Significant Data Fiduciary

CHAPTER III: RIGHTS AND DUTIES OF DATA PRINCIPAL (Sections 11 to 15)

11. Right to access information about personal data
12. Right to correction and erasure of personal data
13. Right of grievance redressal
14. Right to nominate
15. Duties of Data Principal

CHAPTER IV: SPECIAL PROVISIONS (Sections 16 and 17)

16. Processing of personal data outside India
17. Exemptions

CHAPTER V: Data Protection Board of India (Sections 18 and 26)

18. Establishment of Board
19. Composition and qualifications for appointment of Chairperson and Members
20. Salary, allowances payable to and terms of office
21. Disqualifications for appointment and continuation as Chairperson and Members of Board
22. Resignation by Members and filling of vacancy
23. Proceedings of Board
24. Officers and employees of Board
25. Members and officers to be public servants
26. Powers of Chairperson

CHAPTER VI: POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD (Sections 27 and 28)

27. Powers and functions of Board
28. Procedure to be followed by Board

CHAPTER VII: APPEAL AND ALTERNATE DISPUTE RESOLUTION (Sections 29 to 32)

29. Appeal to Appellate Tribunal
30. Orders passed by Appellate Tribunal to be executable as decree
31. Alternate dispute resolution
32. Voluntary undertaking

CHAPTER VIII: PENALTIES AND ADJUDICATION (Sections 33 and 34)

33. Penalties
34. Crediting sums realized by ways of penalties to Consolidated Fund of India

CHAPTER IX: MISCELLANEOUS (Sections 35 to 44)

35. Protection of action taken in good faith
36. Power to call for information
37. Power of Central Government to issue directions
38. Consistency with other laws
39. Bar of jurisdiction
40. Power to make rules
41. Laying of rules and certain notifications
42. Power to amend Schedule
43. Power to remove difficulties
44. Amendments to certain Acts

THE SCHEDULE – Breach types and Penalties

ISACA Chennai Chapter

Legal basis

Personal data can be processed based on

Consent

- Data Principal gives a free, specific, unconditional & unambiguous consent to the Data Fiduciary
- Consents managed by Data Fiduciary or through a Consent manager
- Consent can be withdrawn if Data Principal needs to

Without Consent for the below Legitimate uses

When the Data Principal voluntarily provides

For the State to provide or issue subsidy, benefit, service, certificate, license or permit

For the performance by the State in the interest of sovereignty, integrity, security of the State

For fulfilling obligation under any law (such as employment/labor laws)

For compliance with any judgement or decree or order

For respondent to a medical emergency, provide medical treatment or health services

For taking measures to ensure safety of individuals

ISACA Chennai Chapter

Obligations of the Data Fiduciary

User Journey (or) Data lifecycle

Go to a hotel, share your details and book a room → Hotel stores your personal data, may verify your identity proof → Involves banks for payment processing → Deletes your personal data after X months of stay

- Establish legal basis if consent or Legit
- Collect Personal Data from Data Principals

Process personal data

Involve Data processors

Erase Data

Data Fiduciary obligations

- Provide privacy notice in a clear and plain language
- Have a point of contact for Principals to redress the grievances

- Consent freely given, unconditional & unambiguous
- Obtain parent consent or lawful guardian consent for Children or for a person with disability
- Store consent records

- Do personal data processing
- Implement technical and organizational controls
- Intimate Board on any breaches
- Appoint a DPO
- Do periodic Data Protection Impact assessment
- Appoint a Data auditor for independent data audit

Applicable for significant Data Fiduciaries as determined by the Central Government

- Ensure contractual, technical and organizational controls are in place

- Erase personal data after retention period or upon consent removal

Penalty to Data Fiduciaries for not notifying the breach on timely manner to the Data Principals or the board: May extend up to INR 250 Crores

Penalty to Data Fiduciaries for not meeting children related processing obligations mentioned in the Act: May extend up to INR 250 Crores

Penalty to Significant Data Fiduciaries for not meeting obligations: May extend up to INR 150 Crores

ISACA Chennai Chapter

Measures (indicative)

Technical measures

- **Physical security** – the security relating to premises, keeping equipment's, personnel related etc
- **System security** – the security of your network and information systems, including those which process personal data
- **Data security** – the security of the data you hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely
- **Online security** – eg the security of your website and any other online service or application that you use
- **Device security** – including policies on Bring-your-own-Device (BYOD) if you offer it
- **Data encryption** – through state of the art tools
- **Data pseudonymization** – by reducing personal data footprint
- **Data backup/Archival/deletion** - tooling

Organizational measures

- **Policies** – stating the objectives, responsibilities regarding data protection obligations and alignment to regulatory mandates and company values
- **Notices** – Internal and End customer facing notices based on the channels and data principals
- **Deploying right personnels with responsibilities** – qualified people to run privacy function and other supporting needs on data protection
- **Operating procedures**– to support incident management, individual request rights management
- **Templates/checklists** – to conduct impact assessments
- **Business continuity arrangements** - that identify how you will protect and recover any personal data you hold
- **Periodic checks** - to ensure that your measures remain appropriate and up to date
- **Risk management** – to manage privacy risks

Contractual measures

- **Data Processing Agreements** – as part of contracts
- **Right to audit**– review of the data processor security / privacy processes

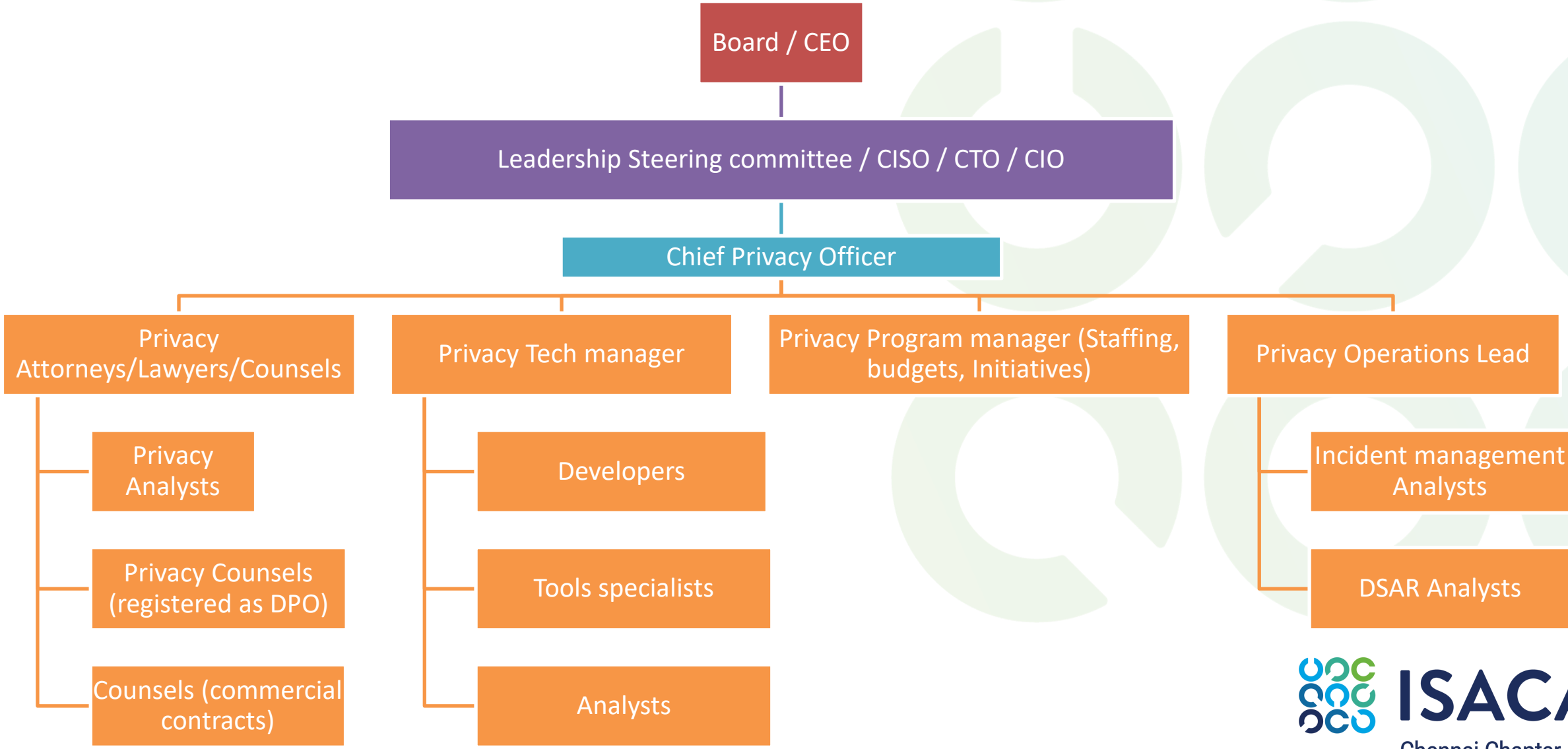
Penalty to Data Fiduciaries for not taking reasonable security safeguards to prevent personal data breach: May extend up to INR 250 Crores

ISACA Chennai Chapter

12 Components of a Privacy Program

ISACA Chennai Chapter

Privacy Program – Org structure for a large global organization



ISACA Chennai Chapter

Typical responsibility

Data Protection Officer

- Is a mandatory role as defined in Section 10 – additional obligations of Significant Data Fiduciary
- Based in India, responsible to governing body of the company; point of contact for grievance redressals
- A DPO may not be an employee of an organization
- DPO role should be independent in assessing privacy issues without any conflict of interest (in deciding the data processing)
- DPO is an advisory function and not for running privacy operations or program

Chief Privacy Officer / Head of Data Privacy

- Is a broader strategic role at leadership level
- Have an active role in managing privacy policies, governance, and compliance
- Runs the privacy program and the privacy operations including appointment of DPOs by region
- Builds synergies with IT, Infosec, Business functions and champion Data privacy and Data protection

Data Protection Board and rules to provide exact requirements

CPO / Head of Data Privacy – an indicative job description

- Develop a global privacy strategy for the organization including its role of a Data controller and processor for Client's personal data
- Responsible for developing organizational privacy policies, SOPs, Guidelines and necessary tooling for organization to embed Privacy into business operations
- Responsible for monitoring and meeting global privacy regulatory obligations with a "risk based" approach
- Ability to forecast and manage a team of privacy specialists who can deliver the program
- Report privacy program progress and seek support from executives
- Manage privacy risks/incidents by demonstrating leadership in driving teams towards data protection authority interactions
- Ability to influence business leaders and other key functions towards the cultural shift of "Privacy first"
- Ability to interact with key clients, vendors and elevate the privacy understanding and demonstrate maturity of the organization
- Participate in industry fraternities and provide a face lift to organization privacy posture

ISACA®
Chennai Chapter

DPDPA 2023

CHAPTER I: PRELIMINARY (Sections 1 to 3)
1. Short title and commencement
2. Definitions
3. Application of Act

CHAPTER II: OBLIGATIONS OF DATA FIDUCIARY (Sections 4 to 10)
4. Grounds of processing personal data
5. Notice
6. Consent
7. Certain legitimate uses
8. General obligations of Data Fiduciary
9. Processing of personal data of children
10. Additional obligations of Significant Data Fiduciary

CHAPTER III: RIGHTS AND DUTIES OF DATA PRINCIPAL (Sections 11 to 15)
11. Right to access information about personal data
12. Right to correction and erasure of personal data
13. Right of grievance redressal
14. Right to nominate
15. Duties of Data Principal

CHAPTER IV: SPECIAL PROVISIONS (Sections 16 and 17)
16. Processing of personal data outside India
17. Exemptions

CHAPTER V: Data Protection Board of India (Sections 18 and 26)
18. Establishment of Board
19. Composition and qualifications for appointment of Chairperson and Members
20. Salary, allowances payable to and terms of office
21. Disqualifications for appointment and continuation as Chairperson and Members of Board
22. Resignation by Members and filling of vacancy
23. Proceedings of Board
24. Officers and employees of Board
25. Members and officers to be public servants
26. Powers of Chairperson

CHAPTER VI: POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD (Sections 27 and 28)
27. Powers and functions of Board
28.Procedure to be followed by Board

CHAPTER VII: APPEAL AND ALTERNATE DISPUTE RESOLUTION (Sections 29 to 32)
29. Appeal to Appellate Tribunal
30. Orders passed by Appellate Tribunal to be executable as decree
31. Alternate dispute resolution
32. Voluntary undertaking

CHAPTER VIII: PENALTIES AND ADJUDICATION (Sections 33 and 34)
33. Penalties
34. Crediting sums realized by ways of penalties to Consolidated Fund of India

CHAPTER IX: MISCELLANEOUS (Sections 35 to 44)
35. Protection of action taken in good faith
36. Power to call for information
37. Power of Central Government to issue directions
38. Consistency with other laws
39. Bar of jurisdiction
40. Power to make rules
41. Laying of rules and certain notifications
42. Power to amend Schedule
43. Power to remove difficulties
44. Amendments to certain Acts

THE SCHEDULE – Breach types and Penalties

ISACA Chennai Chapter

Rights & Duties

Data Principal Rights

Collection
- Right to information
- Right to access personal information

Processing
- Right to consent / withdraw consent
- Right to correct / complete / update

Storage and retention
- Right to erase

Others
- Right to grievance redressal
- Right to nominate

Data Principal duties

- Comply with Law
- Not to impersonate
- Not to suppress information
- Not to register frivolous complaints
- Furnish authentic info, while correcting / erasing

Breach penalty to Data Principals:
May extend up to INR 10,000

ISACA Chennai Chapter

DPDPA 2023

CHAPTER I: PRELIMINARY (Sections 1 to 3)

1. Short title and commencement
2. Definitions
3. Application of Act

CHAPTER II: OBLIGATIONS OF DATA FIDUCIARY (Sections 4 to 10)

4. Grounds of processing personal data
5. Notice
6. Consent
7. Certain legitimate uses
8. General obligations of Data Fiduciary
9. Processing of personal data of children
10. Additional obligations of Significant Data Fiduciary

CHAPTER III: RIGHTS AND DUTIES OF DATA PRINCIPAL (Sections 11 to 15)

11. Right to access information about personal data
12. Right to correction and erasure of personal data
13. Right of grievance redressal
14. Right to nominate
15. Duties of Data Principal

CHAPTER IV: SPECIAL PROVISIONS (Sections 16 and 17)

16. Processing of personal data outside India
17. Exemptions

CHAPTER V: Data Protection Board of India (Sections 18 and 26)

18. Establishment of Board
19. Composition and qualifications for appointment of Chairperson and Members
20. Salary, allowances payable to and terms of office
21. Disqualifications for appointment and continuation as Chairperson and Members of Board
22. Resignation by Members and filling of vacancy
23. Proceedings of Board
24. Officers and employees of Board
25. Members and officers to be public servants
26. Powers of Chairperson

CHAPTER VI: POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD (Sections 27 and 28)

27. Powers and functions of Board
28. Procedure to be followed by Board

CHAPTER VII: APPEAL AND ALTERNATE DISPUTE RESOLUTION (Sections 29 to 32)

29. Appeal to Appellate Tribunal
30. Orders passed by Appellate Tribunal to be executable as decree
31. Alternate dispute resolution
32. Voluntary undertaking

CHAPTER VIII: PENALTIES AND ADJUDICATION (Sections 33 and 34)

33. Penalties
34. Crediting sums realized by ways of penalties to Consolidated Fund of India

CHAPTER IX: MISCELLANEOUS (Sections 35 to 44)

35. Protection of action taken in good faith
36. Power to call for information
37. Power of Central Government to issue directions
38. Consistency with other laws
39. Bar of jurisdiction
40. Power to make rules
41. Laying of rules and certain notifications
42. Power to amend Schedule
43. Power to remove difficulties
44. Amendments to certain Acts

THE SCHEDULE – Breach types and Penalties

ISACA Chennai Chapter

Special Provisions

Cross Border Processing

- Government would notify “Negative list” countries (remember, GDPR works with “White listing” .i.e. Adequacy)
- Stricter law which provides for higher degree of protection (than under DPDPA) will prevail

Exempted processing

- For enforcing Legal Claims
- By judicial and quasi judicial bodies
- For investigation of contravention of law
- For Scheme of arrangement, approved by Tribunal or court
- For ascertaining financial information in the cases of default – IBC

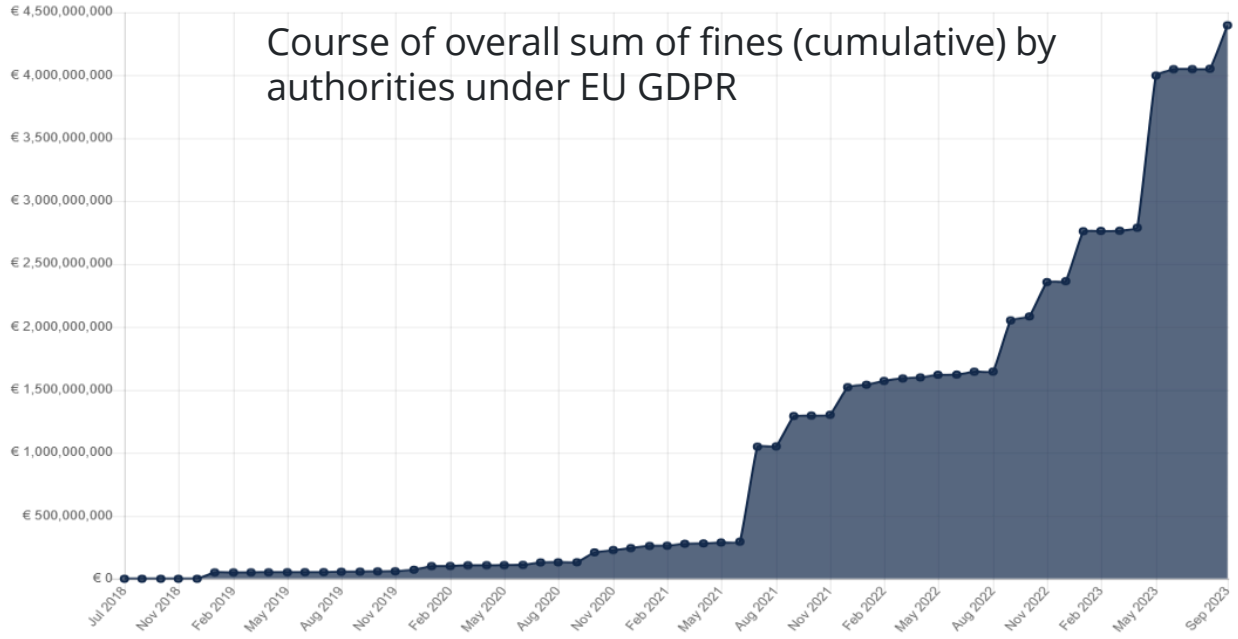
Exempted Persons

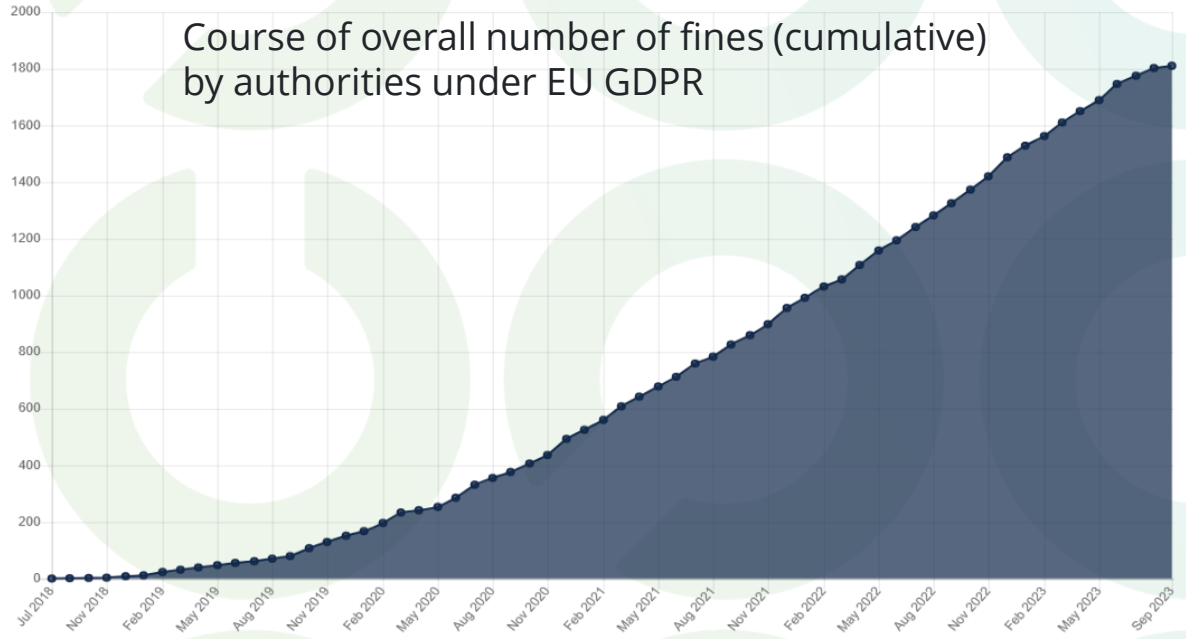
- Government entities - to be notified
- Startups – to be notified – based on volume and nature of data
- Other classes of entities – exempted for specified period – to be notified

ISACA Chennai Chapter

https://www.enforcementtracker.com/

BREAK (from DPDPA)





Sum of Fines by authorities under EU GDPR	
Non-compliance with general data processing principles	**€ 2,025,457,179** (at 483 fines)
Insufficient legal basis for data processing	**€ 1,642,746,672** (at 585 fines)
Insufficient technical and organisational measures to ensure information security	**€ 382,152,575** (at 337 fines)
Insufficient fulfilment of information obligations	**€ 237,275,080** (at 178 fines)
Insufficient fulfilment of data subjects rights	**€ 97,454,970** (at 179 fines)
Unknown	**€ 9,250,000** (at 9 fines)
Insufficient cooperation with supervisory authority	**€ 6,144,029** (at 87 fines)
Insufficient fulfilment of data breach notification obligations	**€ 1,778,582** (at 31 fines)
Insufficient data processing agreement	**€ 1,057,110** (at 11 fines)
Insufficient involvement of data protection officer	**€ 919,300** (at 15 fines)

Number of Fines by authorities under EU GDPR	
Insufficient legal basis for data processing	**585** (with total € 1,642,746,672)
Non-compliance with general data processing principles	**483** (with total € 2,025,457,179)
Insufficient technical and organisational measures to ensure information security	**337** (with total € 382,152,575)
Insufficient fulfilment of data subjects rights	**179** (with total € 97,454,970)
Insufficient fulfilment of information obligations	**178** (with total € 237,275,080)
Insufficient cooperation with supervisory authority	**87** (with total € 6,144,029)
Insufficient fulfilment of data breach notification obligations	**31** (with total € 1,778,582)
Insufficient involvement of data protection officer	**15** (with total € 919,300)
Insufficient data processing agreement	**11** (with total € 1,057,110)
Unknown	**9** (with total € 9,250,000)

Resuming DPDPA 2023

CHAPTER I: PRELIMINARY (Sections 1 to 3)
1. Short title and commencement
2. Definitions
3. Application of Act

CHAPTER II: OBLIGATIONS OF DATA FIDUCIARY (Sections 4 to 10)
4. Grounds of processing personal data
5. Notice
6. Consent
7. Certain legitimate uses
8. General obligations of Data Fiduciary
9. Processing of personal data of children
10. Additional obligations of Significant Data Fiduciary

CHAPTER III: RIGHTS AND DUTIES OF DATA PRINCIPAL (Sections 11 to 15)
11. Right to access information about personal data
12. Right to correction and erasure of personal data
13. Right of grievance redressal
14. Right to nominate
15. Duties of Data Principal

CHAPTER IV: SPECIAL PROVISIONS (Sections 16 and 17)
16. Processing of personal data outside India
17. Exemptions

CHAPTER V: Data Protection Board of India (Sections 18 and 26)
18. Establishment of Board
19. Composition and qualifications for appointment of Chairperson and Members
20. Salary, allowances payable to and terms of office
21. Disqualifications for appointment and continuation as Chairperson and Members of Board
22. Resignation by Members and filling of vacancy
23. Proceedings of Board
24. Officers and employees of Board
25. Members and officers to be public servants
26. Powers of Chairperson

CHAPTER VI: POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD (Sections 27 and 28)
27. Powers and functions of Board
28.Procedure to be followed by Board

CHAPTER VII: APPEAL AND ALTERNATE DISPUTE RESOLUTION (Sections 29 to 32)
29. Appeal to Appellate Tribunal
30. Orders passed by Appellate Tribunal to be executable as decree
31. Alternate dispute resolution
32. Voluntary undertaking

CHAPTER VIII: PENALTIES AND ADJUDICATION (Sections 33 and 34)
33. Penalties
34. Crediting sums realized by ways of penalties to Consolidated Fund of India

CHAPTER IX: MISCELLANEOUS (Sections 35 to 44)
35. Protection of action taken in good faith
36. Power to call for information
37. Power of Central Government to issue directions
38. Consistency with other laws
39. Bar of jurisdiction
40. Power to make rules
41. Laying of rules and certain notifications
42. Power to amend Schedule
43. Power to remove difficulties
44. Amendments to certain Acts

THE SCHEDULE – Breach types and Penalties

ISACA Chennai Chapter

Data Protection Board

- **Data Protection Board of India - Powers and Functions of the Board**:
  - Handling data breaches
  - Investigating complaints
  - Regulating consent managers
  - Conducting Inquiries and Hearings

- **Voluntary Undertaking:** DPB may accept a voluntary undertaking from an entity, outlining actions to address compliance issues, subject to penalties if not followed.

- **Appellate tribunal -** Telecom Disputes Settlement and Appellate Tribunal

- **Bar of Jurisdiction**: Civil courts are barred from entertaining matters within the purview of DPB

- **Alternate Dispute Resolution**: Option for mediation to resolve complaints, promoting a non-adversarial approach to dispute resolution.

ISACA®
Chennai Chapter

DPDPA 2023

CHAPTER I: PRELIMINARY (Sections 1 to 3)

1. Short title and commencement
2. Definitions
3. Application of Act

CHAPTER II: OBLIGATIONS OF DATA FIDUCIARY (Sections 4 to 10)

4. Grounds of processing personal data
5. Notice
6. Consent
7. Certain legitimate uses
8. General obligations of Data Fiduciary
9. Processing of personal data of children
10. Additional obligations of Significant Data Fiduciary

CHAPTER III: RIGHTS AND DUTIES OF DATA PRINCIPAL (Sections 11 to 15)

11. Right to access information about personal data
12. Right to correction and erasure of personal data
13. Right of grievance redressal
14. Right to nominate
15. Duties of Data Principal

CHAPTER IV: SPECIAL PROVISIONS (Sections 16 and 17)

16. Processing of personal data outside India
17. Exemptions

CHAPTER V: Data Protection Board of India (Sections 18 and 26)

18. Establishment of Board
19. Composition and qualifications for appointment of Chairperson and Members
20. Salary, allowances payable to and terms of office
21. Disqualifications for appointment and continuation as Chairperson and Members of Board
22. Resignation by Members and filling of vacancy
23. Proceedings of Board
24. Officers and employees of Board
25. Members and officers to be public servants
26. Powers of Chairperson

CHAPTER VI: POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD (Sections 27 and 28)

27. Powers and functions of Board
28.Procedure to be followed by Board

CHAPTER VII: APPEAL AND ALTERNATE DISPUTE RESOLUTION (Sections 29 to 32)

29. Appeal to Appellate Tribunal
30. Orders passed by Appellate Tribunal to be executable as decree
31. Alternate dispute resolution
32. Voluntary undertaking

CHAPTER VIII: PENALTIES AND ADJUDICATION (Sections 33 and 34)

33. Penalties
34. Crediting sums realized by ways of penalties to Consolidated Fund of India

CHAPTER IX: MISCELLANEOUS (Sections 35 to 44)

35. Protection of action taken in good faith
36. Power to call for information
37. Power of Central Government to issue directions
38. Consistency with other laws
39. Bar of jurisdiction
40. Power to make rules
41. Laying of rules and certain notifications
42. Power to amend Schedule
43. Power to remove difficulties
44. Amendments to certain Acts

THE SCHEDULE – Breach types and Penalties

ISACA Chennai Chapter

Penalties – a recap

Sl. No.	Breach of provisions of this Act or rules made thereunder	Penalty
(1)	(2)	(3)
1.	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (*5*) of section 8.	May extend to two hundred and fifty crore rupees.
2.	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (*6*) of section 8.	May extend to two hundred crore rupees.
3.	Breach in observance of additional obligations in relation to children under section 9.	May extend to two hundred crore rupees.
4.	Breach in observance of additional obligations of Significant Data Fiduciary under section 10.	May extend to one hundred and fifty crore rupees.
5.	Breach in observance of the duties under section 15.	May extend to ten thousand rupees.
6.	Breach of any term of voluntary undertaking accepted by the Board under section 32.	Up to the extent applicable for the breach in respect of which the proceedings under section 28 were instituted.
7.	Breach of any other provision of this Act or the rules made thereunder.	May extend to fifty crore rupees.

On any Data Fiduciary

On Significant Data Fiduciary

On Individuals

On any Data Fiduciary

ISACA Chennai Chapter

Some key next steps towards readiness / implementation

ISACA®
Chennai Chapter

Implementation Readiness – key next steps to begin

- Understand current data processing activities
- Understand Data principals involved, collection purpose, systems involved, location details etc.

Data Mapping

- Monitor DPDPA government notifications
- Analyze the applicability and scope

Monitor DPDPA government notifications

- Develop Program Charter, scope, team structure
- Build synergies with Business and IT teams

Create a Privacy program team

- Allocate resource to analyze DPDPA obligations
- Build mapping to existing privacy capabilities

Expand your current privacy program for DPDPA

- Strengthen the core Data protection tooling / methodologies
- Encryption of data at rest and Transit

Data Protection

- Digital systems to be designed for discovery to support Individual rights requests
- Retention routines

Relook at digital systems

- Understand the data sharing with vendors
- Understand current contract controls

Engaging with Vendors

- Relook at the security incident management tooling / processes

Incident management

- Relook at the SDLC / Release cycles to accommodate Privacy risk assessment stages

Engineering – IT Change management

- Forecast budget for new roles (e.g. DPO, Consent manager)
- Forecast budget for new tooling (consent management platforms, data mapping / discovery tools, Rights request workflow tools)

Risk budgeting

ISACA Chennai Chapter

ISACA®

Chennai Chapter