Deloitte.

The Mauritius Data Protection Act, 2017

Risk Advisory

Private and confidential
March 2019

Contents

1. What is Privacy & Why is it Important ?
2. Existing laws on Privacy
3. Overview and Evolution of Mauritius Data Protection Act, 2017
4. Understanding the Construct of DPA
5. Key Roles under DPA
6. Key Requirements under DPA
7. Annexures- Taking a Deeper View
8. What Next?
9. Deloitte's methodology and approach to DPA

What is Privacy and Why is it Important?

- Promotes that **individuals own their personal data** and not organisations
- **Empowers** an individual to take control of personal data
- Aims to **safeguard personal data** and information that may establish (directly or indirectly) an individual's identity, preferences, activities etc.
- **Governs almost everything** from data creation, processing, storing, and finally destroying.
- **Mandates using individual's data with consent**, for defined purposes and duration

Existing laws on privacy

1

Electronic Transaction Act 2000

Provides the appropriate legal framework to serve as a foundation to facilitate electronic transactions and communications. The Act regulates electronic records and electronic signatures.

2

Banking Act 2004

Requires banks that permit computer access to

- Provide the customers with a privacy policy statement
- Permit any customer to opt out of information sharing concerning him by banks with affiliates and third parties

3

Data Protection Act 2017

Provides for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, manipulate, record or store data relating to individuals.

Overview and Evolution of the Mauritius Data Protection Act, 2017

What is Data Protection Act, 2017 ("DPA")?
The DPA governs privacy rights of individuals in relation to **requirements of collection, processing, storage, transfer and handling of personal information/sensitive personal information**. The formulation of DPA is a response to the requirement of public security, transparent business practices, efficiency in administrations, economic development and growth in technology. The said regulation is seeking to strike a balance between the interests of businesses, Government and the fundamental right to privacy of individuals.
Applicability: The Regulation is applicable to the processing of personal data that is **wholly or partly performed by automated means**. It is applicable to those organizations that are:

a) Established in Mauritius
b) Not established in Mauritius but **uses equipment in Mauritius for processing personal data**, other than for the purpose of transit through Mauritius.

The Regulation is a **sector neutral law** and applies to **all categories of industries.**

Evolution of DPA

DPA 2004 –This Act was formulated to protect individuals with regard to processing of personal data and free movement of such data.

Data Protection Regulation 2009 – Regulations supplementing DPA 2004, formulated to **cater for the registration of data controllers and the relevant fees payable under the Act**. They also comprise of the application for registration/ renewal forms of data controllers and the request for access to personal data forms.

The DPA 2017 came into force on **15th January** 2018 and seeks to strengthen the control and personal autonomy of individuals over their personal data in line with current **relevant international standards, namely the GDPR.**

Understanding the construct of DPA

The DPA in brief

Data Protection Obligation: Personal data should be processed in a manner that is fair, and ensures privacy. It mandates collection and processing of personal data to be limited to a defined purpose

Processing of Personal Data: Principles for processing - a) processed lawfully and fairly, b) data collected for specific purpose, c) adequate and relevant processing, d) keeping the data updated and accurate, e) data kept in a form that permits identification of data subjects only for necessary purpose, and f) processed in alignment with data subject rights

Data Subject Rights: Individuals /or data principals may exercise, a)Right of access, b) Right to Rectification, erasure or restriction of processing , c) Exercise of Rights, d) Right to Object and e) Automated individual decision making

Registration: Registration of controllers and processors with Data Protection Commissioner under PART 3 of DPA. The registration will be for a period not exceeding 3 years and on the expiry of such period, the registration will be cancelled unless the registration is renewed.

Cross border data flow: Cross border transfer of data may take place only if the controller has adduced appropriate safeguards with respect to the protection of personal data to the Data Protection Office or if done under the aegis of the controller, in pursuance of a contract or in public interest.

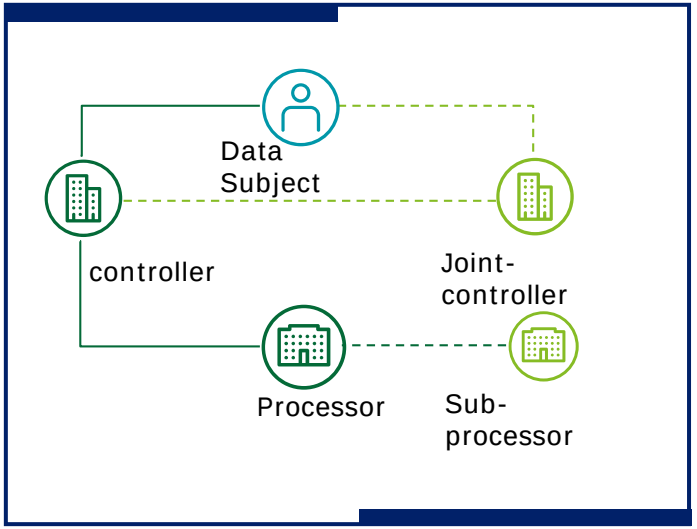
Key roles under DPA

"**Data subject"** means an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, etc. to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual

"**Controller"** means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing

"Joint Controller" together with controller determines the purposes and the means of the processing

"Processor" means a person who, or public body which, processes personal data on behalf of a controller.

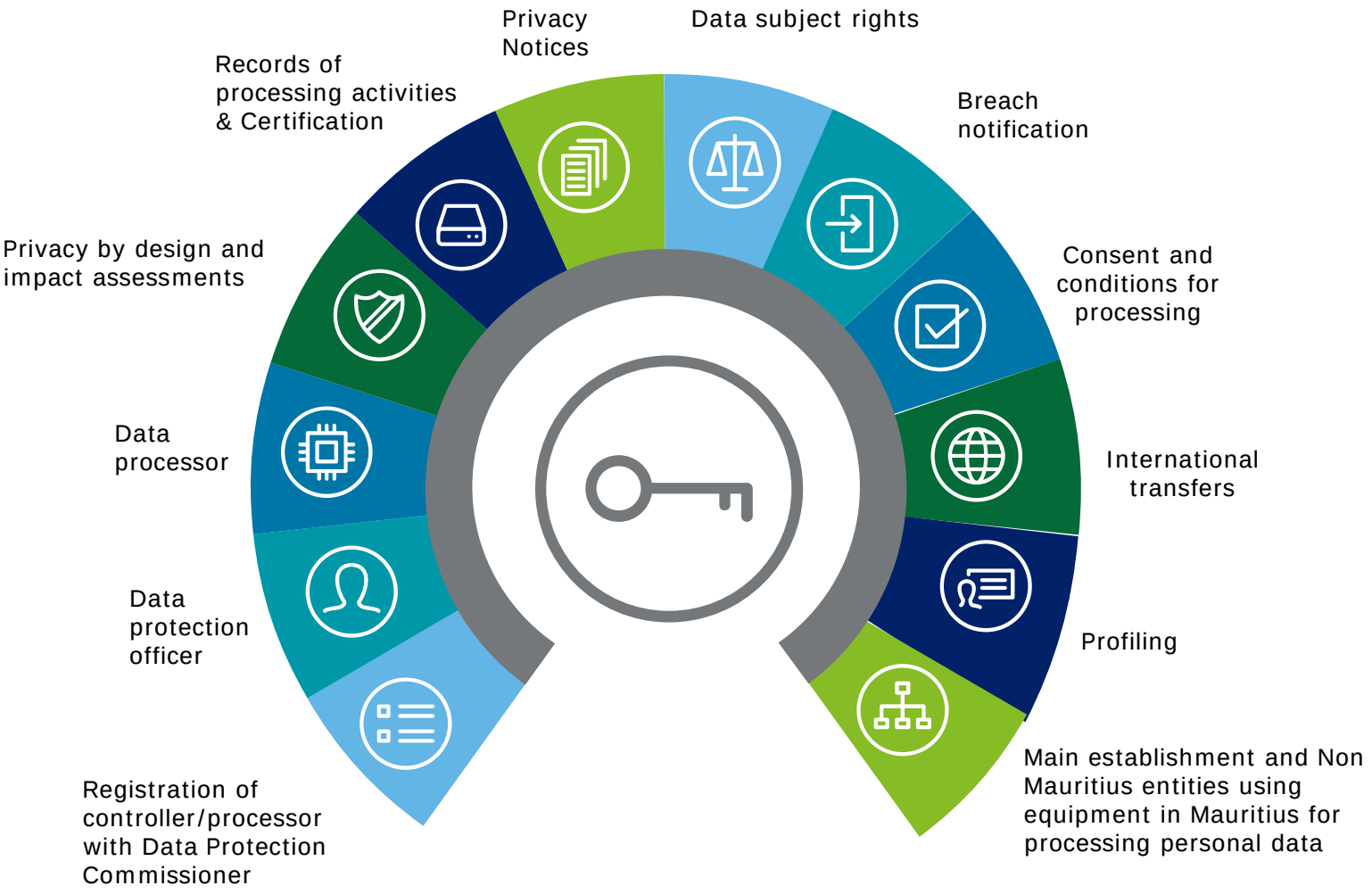


Responsibilities regarding Processors

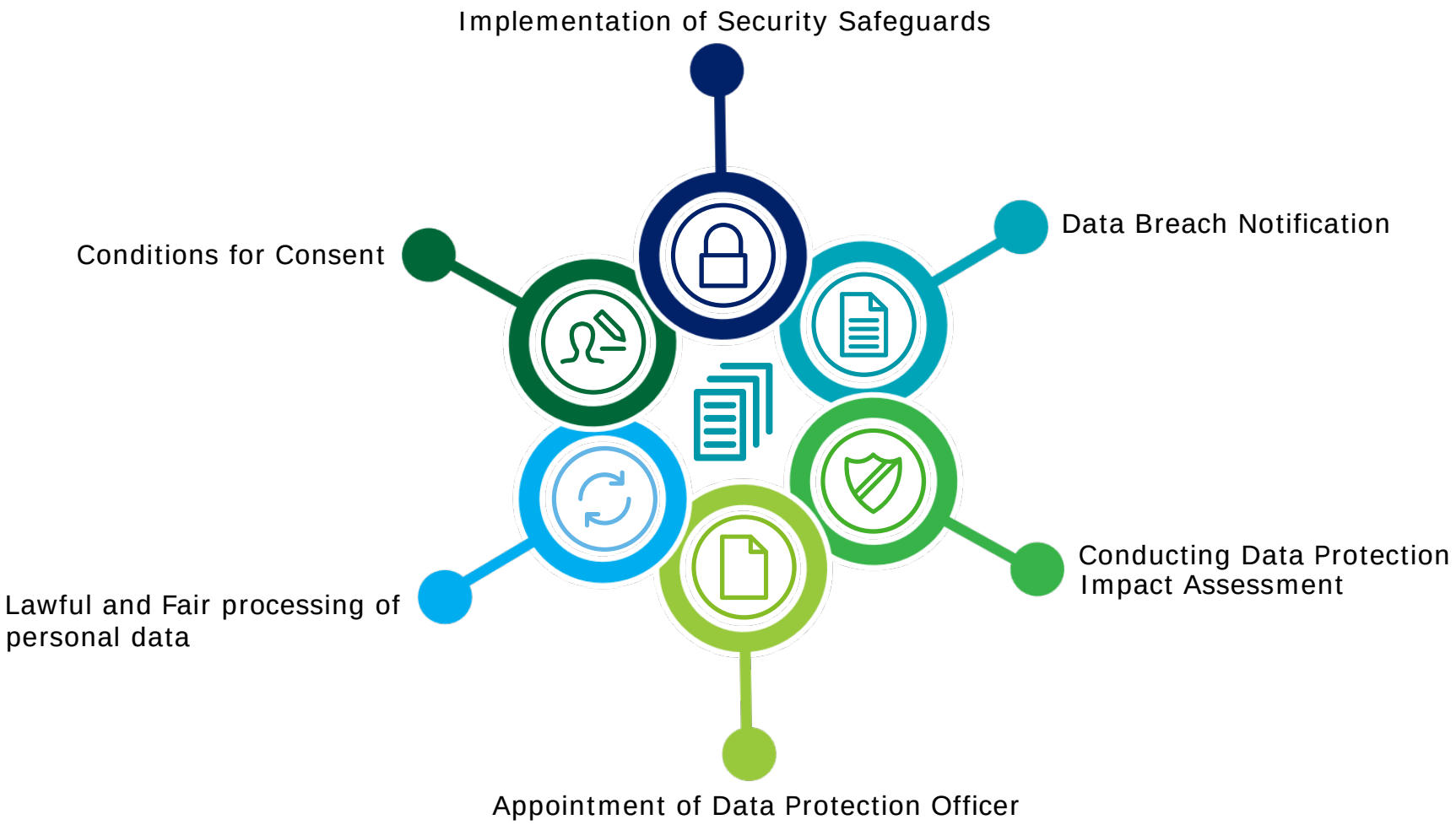
The controller must appoint a processor who offers sufficient guarantees in terms of appropriate technical and organisational measures

- **Assess the processor**
  - Before the start of the contract.
  - On a regular basis (e.g., through audits).
- **Conclude a written agreement with the processor**
  - The DPA specifies minimal information to be included.
- **Set Third party/ sub-contracting conditions**
  - If a processor wants to hire a third party/sub-processor, prior specific or general written consent/instruction of the controller is required.
  - Include a sub-contracting clause in the contract.

Key requirements under DPA



Common Requirements of Mauritius DPA & GDPR:



Key Differences Mauritius DPA and GDPR

Subject Matter	Mauritius DPA	GDPR
Penalties	Fines **up to 200,000 rupees** & **imprisonment up to 5 years**, unless specified otherwise.	Fines range from **2% - 4% of the global annual turnover** of the organization
Data Subject Rights	The **right to data portability is not available.**	**8 Data subject rights** are available
Territoriality	Applies to controller/processors **established in Mauritius** or which uses equipment in Mauritius for processing	Applies to controllers/processors established **both in and outside the EU**
Administrative Fines	Supervisory Authority **cannot** impose fines but the **Court of Law can**	Supervisory Authority has the power to impose fines.
Cross – Border Transfers	Does not include transfer by way of Binding Corporate Rules	Binding Corporate Rules covered

Annexures
Taking a Deeper View

Taking a Deeper View

Key requirements – DPA in a nutshell

1. **Principles relating to processing of personal data-** Controllers/processors need to ensure that processing of personal data is lawful, fair, transparent, accurate and retained for as long as required and proportionate to the purposes for which it is being processed.

2. **Conditions for consent** - Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to them

3. **Notification of a personal data breach** - The controller must notify the breach to the commissioner without undue delay and, where feasible, not later than 72 hours after having become aware of it.

4. **Security of processing**- Measures for ensuring confidentiality, integrity, availability and recovery from failure, Pseudonymisation and encryption must be implemented by organizations.

5. **Prior security check** - Data Protection Commissioner has the power to perform security checks and inspection of the security measures imposed on the controller or processor. This is applicable when the commissioner anticipates a risk to the processing or transfer of personal data.

6. **Data protection officer -** Every controller shall designate an officer responsible for data protection compliance issues. Controller must provide the name and address of the representative who has been nominated for the purposes of DPA in order to seek registration as a controller.

Key considerations:

Record of processing operations- DPA requires the controller/processor to maintain records of their processing activities.

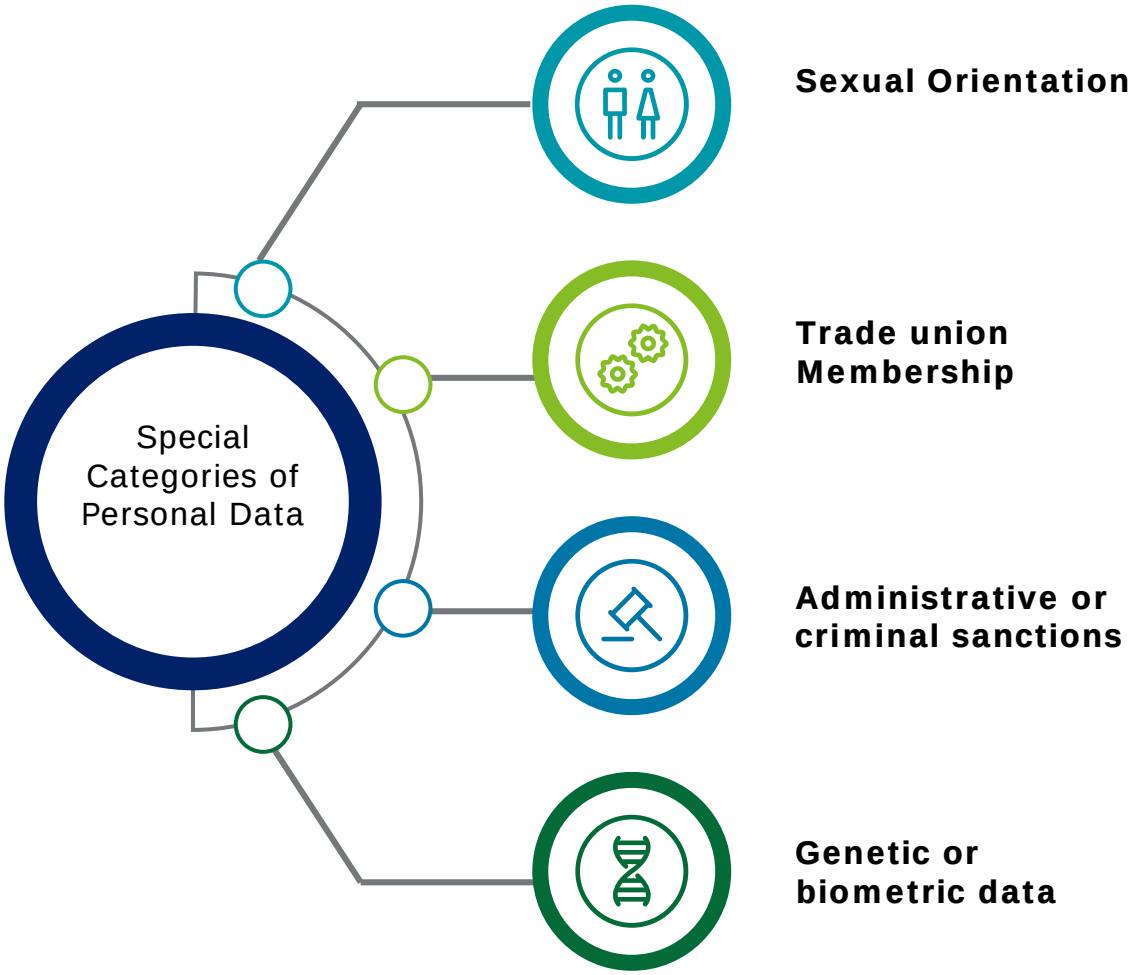
Registration- Registration of controllers and processors with Data Protection Commissioner for a period not exceeding 3 years and on the expiry of such period, the registration will be cancelled unless the registration is renewed.

Cross Border Transfer – Cross border transfer of data may take place only if the controller has adduced appropriate safeguards with respect to the protection of personal data to the Data Protection Office or if done under the aegis of the controller, in pursuance of a contract or in public interest.

Taking a Deeper View

Defining Personal Data & Sensitive Information

- "personal data": Any information relating to a data subject, such as a name, an identification number, location data etc.
- Personal data of a child below the age of 16 years cannot be processed without the consent of child's parents or guardians.
- It is controller's obligation to take every possible measure within the realm of available technology to verify the consent involved in processing a child's data.



Taking a Deeper View

Rights of Data Subjects

01

It is the organization's obligation to put in mechanisms to respond to the requests to data subjects in relation to their rights under privacy regulations within one month of receiving such requests.

02

Organizations' must formulate policies and implement technical solutions to tackle such requests and integrate the policies and tools in their organization by way of technical and administrative safeguards.

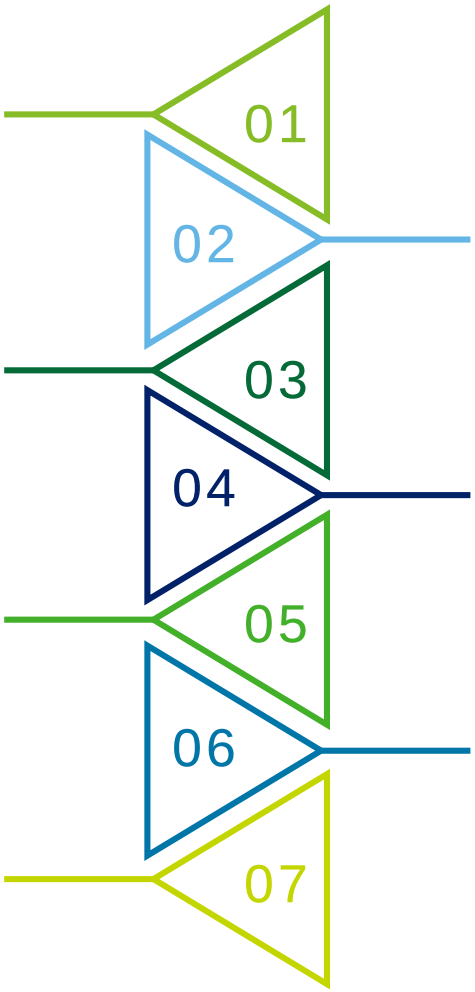
Taking a Deeper View
Rights of Data Subjects

Right to Object:
Three right to object are dealt with in DPA- Processing which is for direct marketing, Processing for scientific/ historic purposes or Processing for legitimate interest.

Right to Rectification:
There may be times when a individual would want the controller to rectify the inaccurate data or maybe to complete the incomplete data with the controller.

Right to Erasure:
The Data Subjects have a right to erasure of data in cases when the data is no longer required and the purpose originally it was taken was has been served or when the data has been unlawfully processed. The right can be exercised against controllers without undue delay and in any event within 1 month.

Right to be Informed:
An individual under DPA has the right to be informed when his/her data is being processed and any other supplemental information with regard to processing. When any such request is generated, the controller must comply without undue delay and within one month.



Right to Access:
The Data Subject, under the Regulation have a right to access their personal data i.e. to a copy and this should be provided free of any charge to the data subject.

Rights in relation to automated decision making and profiling:
The Data Subjects have the right to not to be subject to a decision that is based purely on automated processing and which significantly affects them (example- profiling for jobs, insurance premiums etc.).

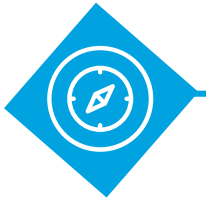
Right to Restrict Processing
Any data can only be processed lawfully under the regulation when consent has been obtained. When a data subject exercises this right to restriction, the Data Controller is obliged to save the data but not to process it unless consented to.

Taking a deeper view

Fines/Penalties and Prosecution and Jurisdiction

Fines and Penalties up to:

200,000 Rupees and Imprisonment for a term not exceeding 5 years



Prosecution and Jurisdiction:

Authorized Officer

An Authorized officer may swear an information in respect to an offence under DPA before a magistrate

Intermediate Court

The intermediate Court will have jurisdiction to try an offence under DPA

Director of Public Prosecution

The Director of Public Prosecution has to give consent to institute any prosecution in relation to DPA

Taking a Deeper View

Security of Processing

Organizations are obligated to factor in appropriate security measures at the time of determining the means of processing data

Implement appropriate security and organizational measures for:

- Prevention of unauthorized access to the data.
- Ensure that the measures provide a level of security appropriate for the harm that might result from a breach and the nature of data concerned.

Security measures should include:

- Pseudonymisation and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- The ability to periodically test the effectiveness of the security measures

The security measures should be implemented keeping in mind the state of technology available, financial considerations, nature of data processed and risks associated with processing data

Using services of a processor:

- A processor should be chosen if sufficient guarantees are provided regarding organizational and security measures at the processors end.
- The controller and processor should enter into a written contract entailing that processor to act only on the written instructions of controller and obligation on processor to comply with security and organizational measures related compliances.

Prior security check:

- If the commissioner believes that there is a specific risk to the privacy rights of data subjects, then an audit or an inspection may be conducted prior to processing or transfer of data.
- The audit or inspection would be undertaken to assess the security measures implemented to safeguard the processing or transfer of data.

Taking a Deeper View

Data Protection Impact Assessment

Data protection impact assessments (DPIAs) help organizations identify, assess and mitigate or minimize privacy risks with data processing activities. They're particularly relevant when a new data processing process, system or technology is being introduced.

DPIA is strictly required in the following cases:

01 A systematic and extensive evaluation of personal aspects which is based on automated processing, including profiling, and on which decisions are based that produce legal effects or similarly significantly affect the natural person.

02 Processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences.

03 A systematic monitoring of a publicly accessible area on a large scale.

DPIA should at least contain these:

01 A systematic description of the envisaged processing operations and the purposes of the processing

02 An assessment of the necessity and proportionality of the processing operations in relation to the purposes

03 An assessment of the risks to the rights and freedoms of data subjects

04 The measures envisaged to address the risks, including safeguards, security measures and mechanisms.

Taking a deeper view
Data breach notifications

Organisations will have to:

1. notify the Commissioner of a breach 'without undue delay' not later than 72 hours. Processor to notify the controller 'without undue delay'..
2. notify the data subjects if the breach is likely to affect the privacy, rights or legitimate interests of an individual.
3. keep an internal register of the data breaches that have occurred in the organization.

The obligation to notify individuals may, at the discretion of the regulator, be dropped, if the organisation can prove that it has taken appropriate means to prevent adverse effects on individuals.

Personal data breaches can result in high risks for the rights and freedoms of individuals

E.g. Discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, etc.

Taking a Deeper View

Miscellaneous

Right of Appeal: A person aggrieved by a decision made by the commissioner can appeal to the Tribunal within 21 days from the date of the decision.

Duty to Destroy Personal Data: Post lapse of purpose of collecting personal data, the controller should destroy the data as soon as reasonably possible and notify the processor holding the data.

Compliance Audit: The commissioner may carry out periodical audits of the systems of controllers or processors to ensure compliance under DPA.

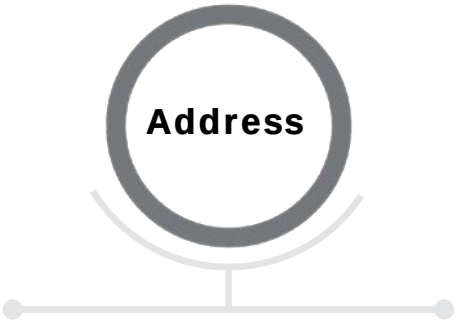
Certification: The certification is voluntary and will be valid for 3 years. The data protection office will lay down technical standards to be met with to procure the certificate

Summary

Three step conclusion to address the current situation:

- Identify and empower an individual within your organization to be the contact point (internal, external, regulatory), to monitor, report and plan for changing legal obligations and establish consistent messaging.
- Gather existing documentation on data processing operations, including data transfers, to evaluate risk exposure and prepare for potential inquiries from stakeholders like the Authority (to be established), clients or employees etc.

- Develop an inventory of systems, controls, and procedures to understand where personal data are processed and which specific controls (e.g., data usage) exist.
- Assess available cross border transfer methods and shortlist the method(s) that meet the requirements of your organization.
- Assess your current state



- Communicate regulatory changes and their potential impact to senior stakeholders to raise awareness and obtain senior-level support.
- Develop a risk based remediation strategy and roadmap including a short term tactical plan focusing on “quick wins”.
- Develop and execute a communications plan.

What Next?

Taking a Deeper View

A Proactive approach can help

Organizations may consider following initiatives:

01 Privacy Readiness Assessment

02 Define Personal and Sensitive Personal Data

03 Create Inventory of Personal and Sensitive Personal Data

04 Understand data flows for collection & processing of personal data

05 Develop culture of privacy with awareness and training session

06 Establish a robust framework on leading privacy principles

07 Establish and/or update information notice and consent mechanisms

08 Enhance data security measures

09 Include Privacy as a measure for risk assessment of third parties

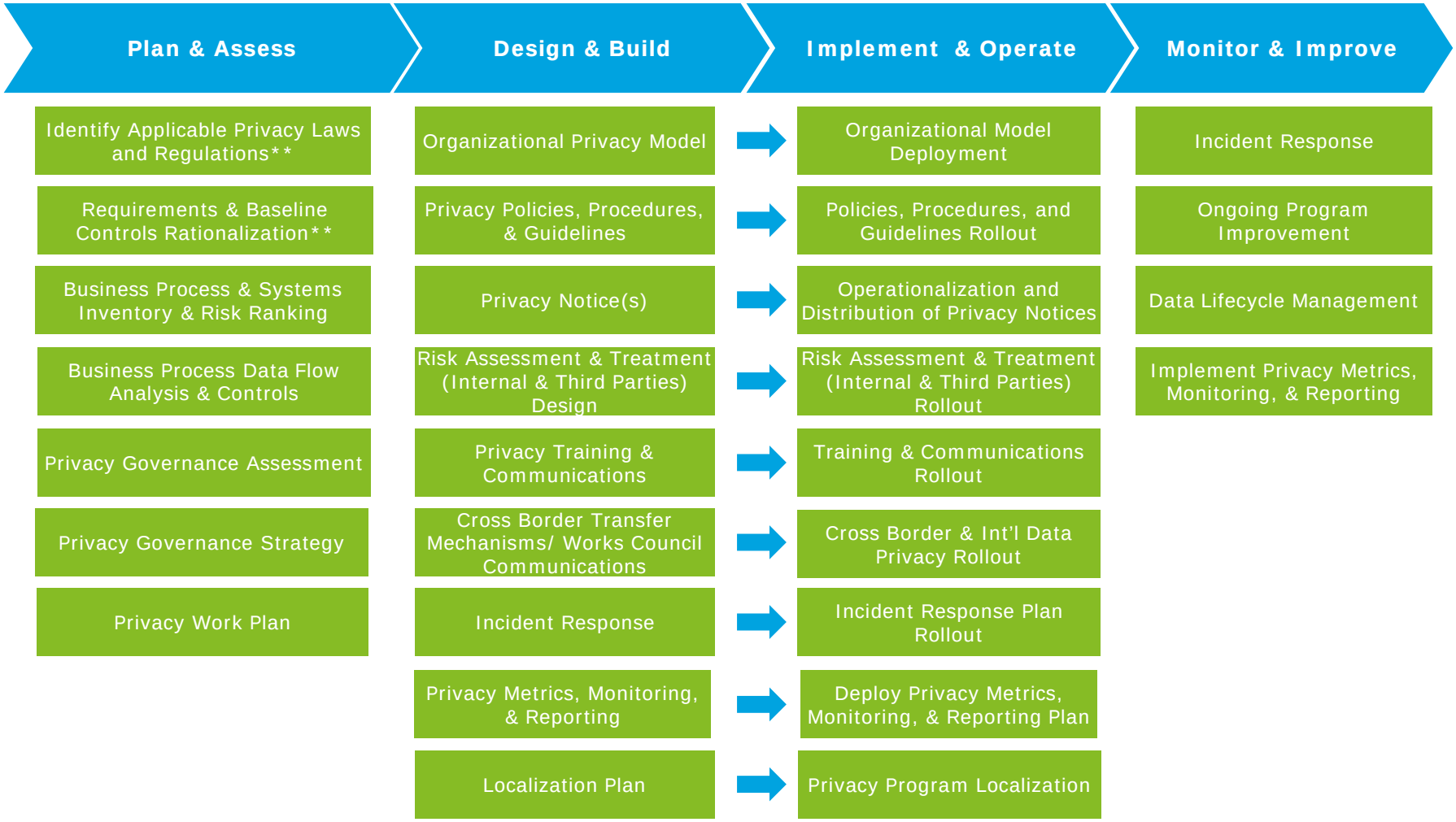
10 Assess the website

11 Assess the Third party data lifecycle activities which they conduct

12 Review contracts

Deloitte’s methodology and approach to DPA

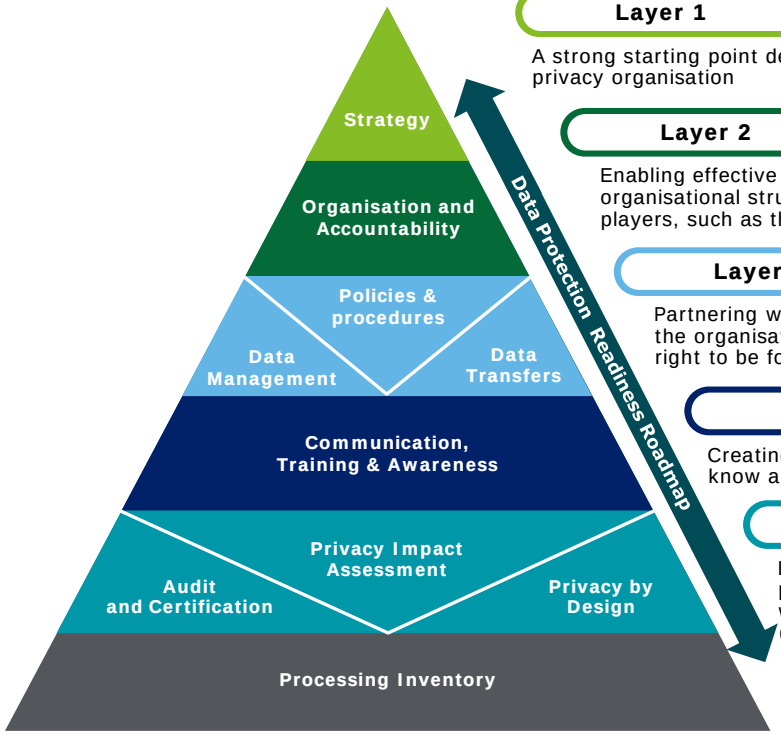
Deloitte's time-tested privacy Methodology



Road to maturity

Deloitte's holistic privacy programme defines six layers that can add value in the development of privacy within an organisation

A tailored transformation programme helps organisations prepare in the optimal for privacy compliance



Layer 1 STRATEGY

A strong starting point determining high level direction and risk appetite, upon which the organisation builds its privacy organisation

Layer 2 ORGANISATION AND ACCOUNTABILITY

Enabling effective implementation of the privacy strategy requires a strong and multidisciplinary privacy organisational structure. This covers the structure of the privacy organisation as well as the role and position of key players, such as the Data Protection officer. This layer also covers accountability; how to prove compliance?

Layer 3 POLICY, PROCESS & DATA

Partnering with the Business to realise data is protected, governed, managed and utilised effectively in line with the organisation's strategy. Also covers technological challenges such as data access requests, data retention, right to be forgotten, breach notification and international and third party data transfers.

Layer 4 CULTURE, TRAINING & AWARENESS

Creating a high level of organisational awareness on privacy realises that the organisation's employees know and follow the rules.

Layer 5 PRIVACY OPERATIONS

Embedding privacy into the organisations project methodology. This is done by efficient and practical guidance during conception of a new or changed product or service (Privacy by Design) as well as assessing new and existing systems following the established Privacy Impact Assessment (PIA) method

Layer 6 PROCESSING INVENTORY

A processing inventory is a fundamental element of any privacy programme, and will be a mandatory requirement from the GDPR

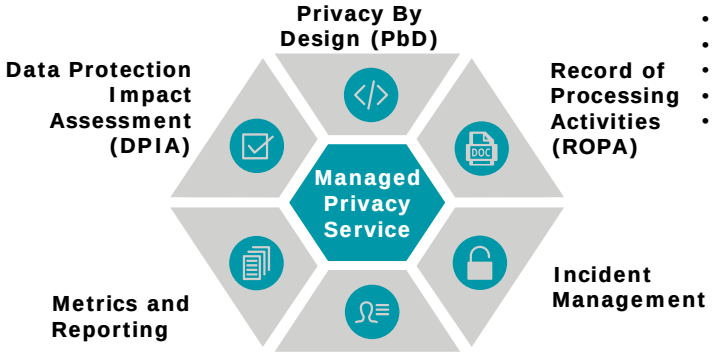
Privacy and Data Protection (PDP) capabilities

PDP capabilities

Privacy capabilities

- Privacy Programme Assessments
- Privacy Operational Assessments
- Privacy Programme Development
  - Privacy policies and notices
  - Privacy programme training
  - Privacy Governance Model Design
  - Privacy Incident Response
- Privacy Programme Implementation
- Rationalisation of requirements
- Data Discovery via tools and Data Flow Diagrams
- Advisory as per existing and new/upcoming laws

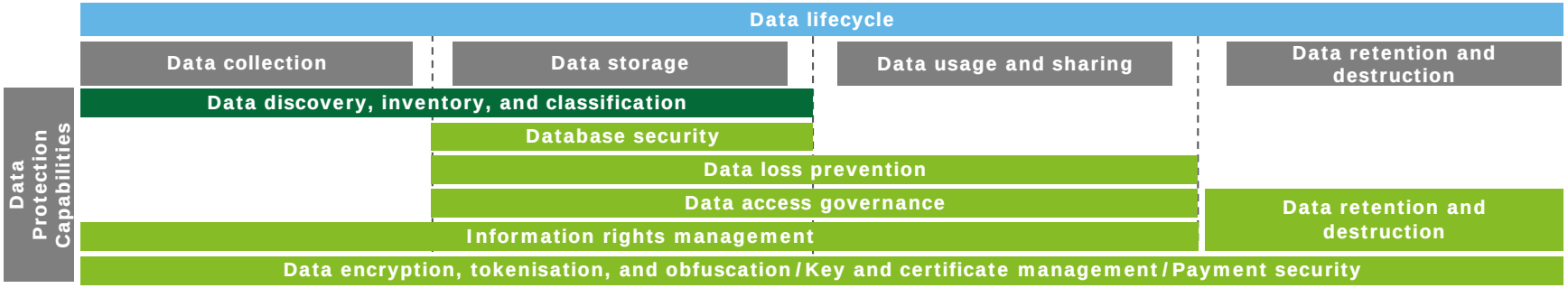
Managed privacy services



Privacy assessment capabilities

- Privacy Readiness Assessment
- Data Discovery via tools and Data Flow Diagrams
- Preparation of Data Flow Diagrams
- Data Protection Impact Assessment
- Post implementation review
- Training and workshops
- Privacy Remediation
  - Privacy By Design
  - Breach readiness
  - Data Subject Access Rights
  - Consent Management

Data Protection Capabilities



Deloitte's GDPR Experience- Global

		Industries					
FY	**Project Type**	**Consumer & Industrial Products**	**Energy & Resources / Public sector / Others**	**Financial Services**	**Life Sciences & Health Care**	**Technology, Media & Telecommunications**	**TOTAL***
FY18	Readiness Assessment	35	3	12	9	24	83
	Program Design & Implementation	39	10	31	23	44	147
FY17	Readiness Assessment	8	-	1	4	2	15
	Program Design & Implementation	10	-	1	5	7	23
	TOTAL	92	13	45	41	77	268

Deloitte.