THE EU GENERAL DATA PROTECTION REGULATION (GDPR) AND THE DATA PROTECTION ACT 2017

By Rushda Goburdhun
Data Protection Office

Agenda

- EU Directive 95/46/EC
- EU GDPR
  - GDPR structure
  - Key changes
- The Data Protection Act 2017 (DPA)
- Relationship between DPA and GDPR
- Similarities between DPA and GDPR
- GDPR and DPA checklist

EU Directive 95/46/EC

Prior to the GDPR, the EU's data protection regime was governed by this Directive.

The Directive (as with all EU Directives) did not apply automatically, and had to be transposed into the national laws of each Member States.

Inevitably, the national legislatures of the Member States applied their own interpretation of the Directive, resulting in non identical data protection compliance requirements across the EU.

EU GDPR

A single framework for data protection legislation across the EU which came into force on **25 May 2018**.

Contains 173 introductory clauses (Recitals), 11 chapters and 99 Articles.

It protects the fundamental rights and freedoms of data subjects and enable the free movement of personal data within the EU.

GDPR Structure

Chapter 1	• General Provisions (Art. 1 to 4)
Chapter 2	• Principles (Art. 5 to 11)
Chapter 3	• Rights of the Data Subject (Art. 12 to 23)
Chapter 4	• Controller and Processor (Art. 24 to 43)
Chapter 5	• Transfer of Personal Data to 3rd Countries or International Organizations (Art. 44 to 50)
Chapter 6	• Independent Supervisory Authorities (Art. 51 to 59)
Chapter 7	• Cooperation and Consistency (Art. 60 to 76)
Chapter 8	• Remedies, Liability and Penalties (Art. 77 to 84)
Chapter 9	• Provisions Relating to Specific Processing Situations (Art. 85 to 91)
Chapter 10	• Delegated Acts and Implementing Acts (Art. 92 to 93)
Chapter 11	• Final Provisions (Art. 94 to 99)

Key Changes

Territorial Scope (extra-territorial applicability)

- GDPR applies to both controllers and processors established in the EU, as well as those outside the EU, who offer goods or services to, or monitor EU data subjects.

Consent

- Stricter regime on consent.
- Controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Accountability

- The GDPR introduces a new concept of accountability, which requires an organisation to demonstrate how it complies with the GDPR.
- Example: Keeping records of processing, implementing appropriate safeguards amongst others

Key Changes

Transparency

- The GDPR increases the amount of information that a controller must provide to data subjects when collecting their personal data, to ensure that the processing activities are fair and transparent.
- Controllers must provide the information in an easily accessible form, using clear and plain language.

Processors

- GDPR imposes direct obligations on processors.
- Processors are also directly required to comply with a number of specific obligations, including to maintain adequate documentation (Article 30), implement appropriate security standards (Article 32) amongst others.

Higher bar for Lawful Processing

- The GDPR includes new limitations on the use of consent as a ground for processing.
- There are six lawful basis for processing.
- Which basis is most appropriate to use will depend on the organisation purpose and relationship with the individual.

Key Changes

Breach Notification

- Mandatory obligation to notify the personal data breach to the supervisory authority within 72 hours after having become aware of it, unless the controller is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Rights of data subjects

- The GDPR provides individuals with new and enhanced rights, including the right to data portability, and the right not to be subject to a decision based on profiling, in certain circumstances.

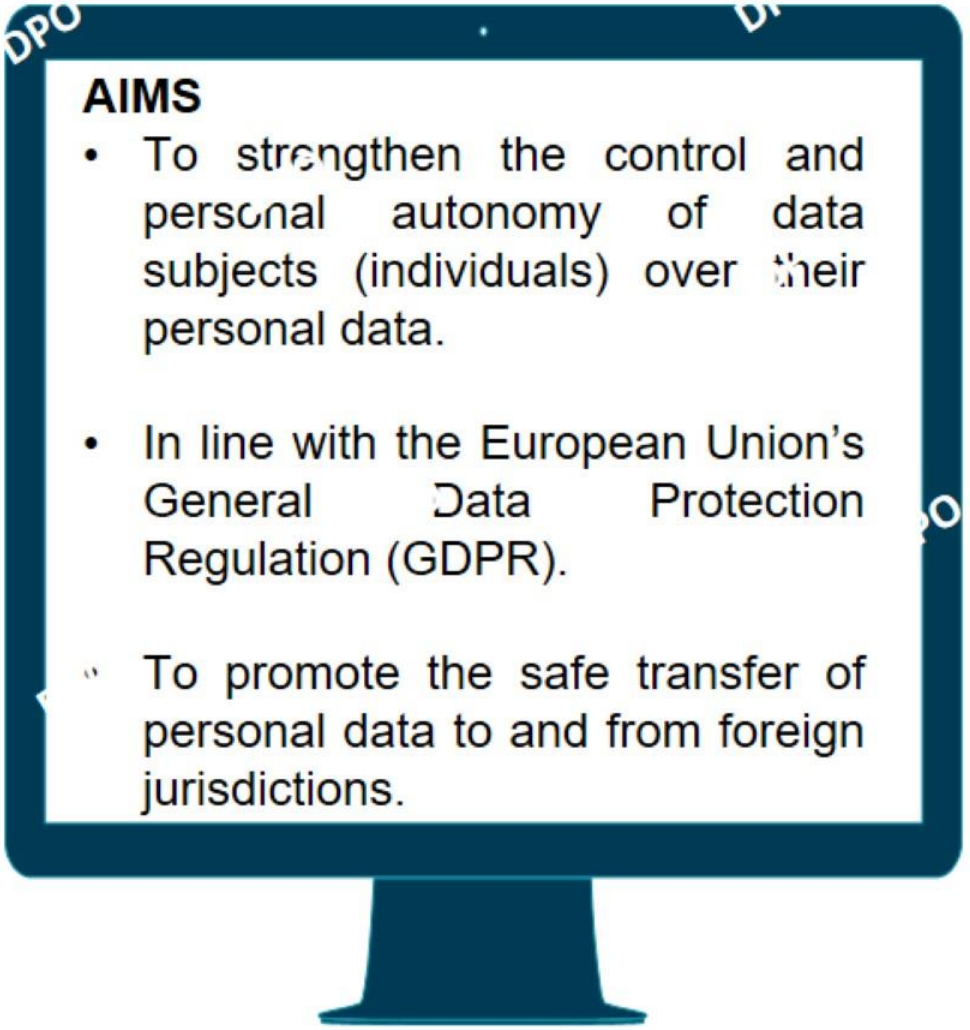
Remedies and sanctions

- Failure to comply with the GDPR can result in heavy fines.
- A maximum of €20,000,000 or 4% of global turnover, whichever is the higher.

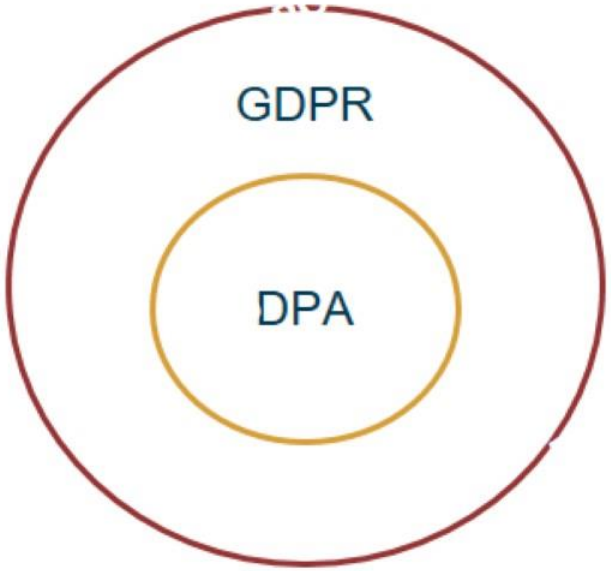
THE DATA PROTECTION ACT 2017

THE DATA PROTECTION ACT 2017

(Came into force on 15 January 2018)



Relationship between GDPR and DPA



- **DPA is a subset of GDPR.**
- **That is, it has incorporated those principles of GDPR which are applicable in the Mauritian Context.**

SIMILARITIES BETWEEN DPA AND GDPR

DPA (Section)	GDPR (Article)
6 - Investigation of complaints Amicable settlement of disputes and conduct of hearings has been included.	40 - Codes of conduct (2)(k)
21- Principles relating to processing of personal data	5 - Principles relating to processing of personal data
22 - Duties of controller	24 - Responsibility of the controller
23 – Collection of personal data	13 - Information to be provided where personal data are collected from the data subject
24 - Conditions for consent	7 - Conditions for consent
25 - Notification of personal data breach	33 - Notification of a personal data breach to the supervisory authority
26 - Communication of personal data breach to data subject	34 - Communication of a personal data breach to the data subject

DPA (Section)	GDPR (Article)
28 - Lawful processing	6 - Lawfulness of processing
29 - Special categories of personal data	9 - Processing of special categories of personal data
30 - Personal data of child	8 - Conditions applicable to child's consent in relation to information society services
31 - Security of processing	28 - Processor 29 - Processing under the authority of the controller or processor 32 - Security of processing
33 - Record of processing operations	30 - Records of processing activities
34 - Data protection impact assessment	35 - Data protection impact assessment
35. Prior authorisation and consultation	36 - Prior consultation

DPA (Section)	GDPR (Article)
36 - Transfer of personal data outside Mauritius	46 - Transfers subject to appropriate safeguards 49 - Derogations for specific situations
37 - Right of access	15 - Right of access by the data subject
38 - Automated individual decision making	22- Automated individual decision-making, including profiling
39 - Rectification, erasure or restriction of processing	16 - Right to rectification 17 - Right to erasure ('right to be forgotten') 18 - Right to restriction of processing
40 - Right to object	21 - Right to object
44 – Exceptions and Restrictions	23 - Restrictions
49 - Certification	42 - Certification

GDPR AND DPA CHECKLIST

Checklist – Q1

Are you complying with the 6 principles relating to personal data processing?

- Organisations must ensure that their processing activities comply with all of the Data Protection Principles set out in Article 5 of the GDPR and section 21 of the DPA.
- Example:
  - the purpose limitation principle;
  - the principle of data minimisation;
  - data retention;
  - in accordance with the rights of data subjects; etc.).

Checklist – Q2

Are you complying with the lawfulness of processing rules?

- Organisations should:
  - in relation to each type or category of processing, ensure that they have identified and documented the grounds for lawful processing
  - and where the legitimate interests ground is being used, document what the legitimate interests are.
- Given the new limitations around consent, ensure that consent is used as a ground only where it is the only way to justify that processing.

- Article 6 GDPR
- Section 28 of the DPA

Checklist – Q3

Do you have procedures in place to review how you obtain, record and manage consent?

- The GDPR as well as the DPA set a high standard for consent.
- The obligations of an organisation don't end when it first get consent. The company should continue to review consent as part of its ongoing relationship with individuals, not a one-off compliance box to tick and file away.
- The data subject shall have the right to withdraw his or her consent at any time. Have procedures in place to deal with withdrawal of consent

- Article 7 of GDPR
- Section 24 of DPA

Checklist – Q4

Transparency and information to be provided. Has your organisation provided to individuals information regarding the use of their personal data?

- Individuals need to know that you are collecting their data, why you are processing it and who you are sharing it with.
- You should:
  - consider the best process to provide such information in a clear and intelligible form
  - update employee and customer notices to take account of the new requirements.

- Article 13 of GDPR
- Section 23 of DPA

Checklist – Q5

Has your organisation documented what personal data it holds, where it came from, who the company share it with and what the organisation do with it?

It is mandatory for an organisation to maintain a record of all processing operations under his or its responsibility according to section 33 (1) of the DPA and Article 30 of GDPR.

Checklist – Q6

Do you have a process to effectively identify, report, manage, resolve any personal data breaches and communicate to data subject where necessary?

- Organisations should:
  - put in place data breach response and notification procedures to meet 72 hour deadlines in respect of notifications to the Supervisory Authority i.e. Data Protection Office;
  - put in place data breach response procedures to evaluate situations exposing data subjects to high risk and procedures to enable notifications to be made to data subjects "without undue delay" in such circumstances;
  - maintain a personal data breach register.

- Articles 33 and 34 of GDPR
- Sections 25 and 26 of DPA

Checklist – Q7

Have you implemented security measures for protecting personal data you process?

- Before deciding on what level of security is right for your business, you need to review the personal data you hold and assess the risks to that information.
- It is recommended to have an **Information security policy.** The policy should clearly set out the approach to security together with responsibilities for implementing it and monitoring compliance.
- It is good practice to identify a person or department in the business with day-to-day responsibility for developing, implementing and monitoring its security policy.

- Article 32 of GDPR
- Section 31 of DPA

Checklist – Q8

Have you conducted data protection impact assessments where necessary?

- Controllers must carry out data protection impact assessments where the processing is likely to result in a high risk to the rights and freedoms of individuals.
- Organisations should:
  - have in place a process for determining whether a DPIA is required;
  - if they come to the conclusion that DPIA is not required, document the decision properly.

- Article 35 of GDPR
- Section 34 of DPA

Checklist – Q9

Do you have policies, processes and procedures to ensure, right of access; rectification ,erasure and restriction of processing by the data subject?

- Individuals have the right to:
  - access their personal data and supplementary information;
  - not to be subject to a decision based solely on automated processing which significantly affect them (including profiling);
  - have their personal data rectified if it is inaccurate or incomplete;
  - have personal data erased and to prevent processing in specific circumstances.
- Organisations should thus have procedures in place to deal with data subjects' rights.

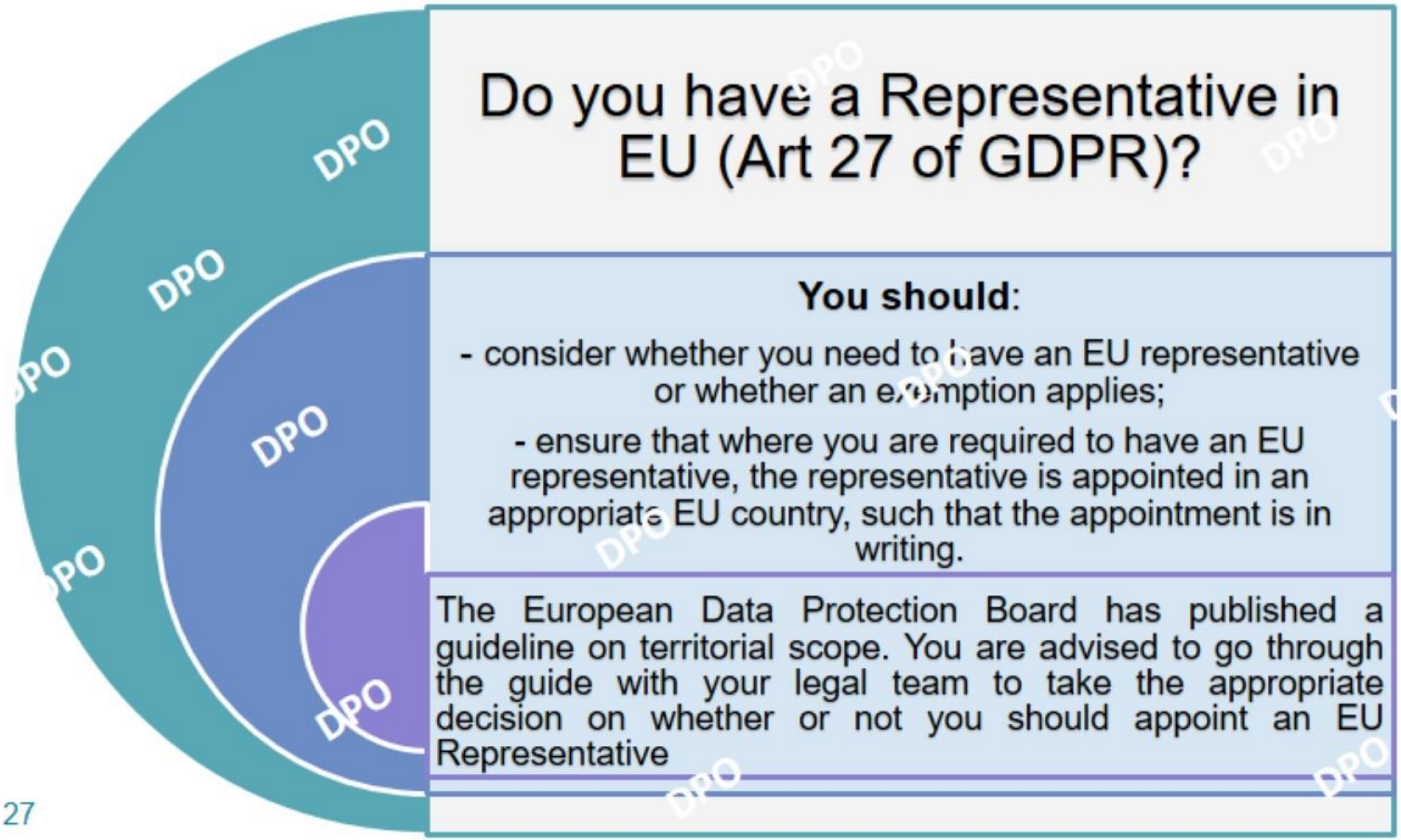
- Article 15 – 18 of GDPR: Right of access; to rectification; to erasure; to restriction of processing
- Section 37-40 of DPA

Checklist – Q10

Has your organisation appointed an appropriate data protection officer(dpo) following the EU requirements and DPA?

It is mandatory for an organisation to appoint a data protection officer under section 22 (e) of the DPA while for GDPR it is only under certain circumstances that controllers and processors need to appoint a dpo. (see Articles 37-39 of the GDPR).

Checklist – Q11



Do you have a Representative in EU (Art 27 of GDPR)?

You should:

- consider whether you need to have an EU representative or whether an exemption applies;
- ensure that where you are required to have an EU representative, the representative is appointed in an appropriate EU country, such that the appointment is in writing.

The European Data Protection Board has published a guideline on territorial scope. You are advised to go through the guide with your legal team to take the appropriate decision on whether or not you should appoint an EU Representative

Example 1

- A website, based and managed in Turkey, offers services for the creation, edition, printing and shipping of personalised family photo albums. The website is available in English, French, Dutch and German and payments can be made in Euros or Sterling.
- The website indicates that photo albums can only be delivered by post mail in the UK, France, Benelux countries and Germany.

GDPR applies as per Article 3 (2)(a)

- In this case, it is clear that the company is providing a service to EU data subjects. The fact that the website is available in four languages of the EU and that photo albums can be delivered by post in six EU Member States demonstrates that there is an intention on the part of the Turkish website to offer its services to individuals in the Union.

In accordance with Article 27, the controller will have to designate a representative in the Union.

Example 2

- **A marketing company established in the US provides advice on retail layout to a shopping centre in France, based on an analysis of customers' movements throughout the centre collected through Wi-Fi tracking.**

GDPR applies as per Article 3 (2)(b)

- The analysis of a customers' movements within the centre through Wi-Fi tracking will amount to the monitoring of individuals' behaviour. In this case, the data subjects' behaviour takes place in the Union since the shopping centre is located in France.

In accordance with Article 27, the controller will have to designate a representative in the Union.

Example 3

- **A private company based in Monaco processes personal data of its employees for the purposes of salary payment. A large number of the company's employees are French and Italian residents.**

The private company is not subject to the provisions of the GDPR.

- While the processing carried out by the company relates to data subjects in France and Italy, it does not takes place in the context of an offer of goods or services.
- Human resources management, including salary payment by a third-country company cannot be considered as an offer of service within the meaning of Art 3(2)a.

Example 4

- A bank in Taiwan has customers that are residing in Taiwan but hold German citizenship.
- The bank is active only in Taiwan; its activities are not directed at the EU market. The bank's processing of the personal data of its German customers is not subject to the GDPR.

Example 5

- The Canadian immigration authority processes personal data of EU citizens when entering the Canadian territory for the purpose of examining their visa application. This processing is not subject to the GDPR.

Checklist – Q12

Have you implemented safeguards for transfers outside Mauritius and/or cross border transfers for EU?

You should:

- Identify all conditions in which personal data are transferred to recipients located abroad;

-Inform data subjects of eventual transfer where necessary.

- Implement appropriate safeguards for the transfer. The onus lies on you to ch0ose the required security measures for the transfer.

Articles 44 to 49 of GDPR
Section 36 of DPA

THANK YOU!