Record of processing operations

Record of processing operations

What does the Act say?

"Every controller or processor shall maintain a record of all processing operations under his or its responsibility." ***(section 33 of the DPA)***

Record of processing operations

Understand what records to keep

- Records of processing activities, such as:
  - personal data you hold;
  - where it came from?;
  - how you share it?
- Information audit across your organisation / specific business areas;
- Access to personal information are performed with a particular business purpose.

Record of processing operations

What records to keep?

Contact details of controller / processor

any Data Protection Officer / Representative (where applicable)

Purpose of processing

a list of the types of purposes

Description of personal data

personal data being kept / processed

Record of processing operations

What records to keep?

Categories of data subjects

the functional data categories

Name of processor

for the processing activity (where applicable)

Recipient categories

what categories of recipients are involved (where appropriate)

Record of processing operations

What records to keep?

Transfer of data outside Mauritius

countries / international organisations involved in the data transfer

Documents for appropriate safeguards

list the documents that clarify the appropriate safeguards & where these documents are stored

Description of mitigating measures

provide a general statement and list the 'standard measures'

Record of processing operations

What records to keep?

Retention period

provide the retention period for the processed data

Effectiveness of policies & mechanism verification - section 22(3)

- training of employees on data protection
- number of incidents
- statistics of controls in place

Record of processing operations

What records to keep?

Case scenario

- An organisation has the following business operations where personal data are processed: 1) sales / invoicing, 2) marketing & 3) finance

Analysis

- After carrying out an audit of the personal data processed, 3 rows of business process, respectively, have to be filled for the compulsory fields *(as illustrated above)*

Record of processing operations

How will these records help you?

- **Such records may be considered as one of the tools enabling the Data Protection Officer to perform his / her tasks of:**
  - **monitoring compliance;**
  - **informing and advising the controller / processor.**

- **A fine-grained audit trail must be implemented so that unauthorised access can be traced easily.**

Case scenario

- If you have inaccurate personal data and have shared this with another organisation, you will have to inform the other organisation about the inaccuracy so that it correct its own.

Record of processing operations

Main Points & To do list

Records	Audit	Data Protection Office
Keeping records of processing operation is compulsory.	**Carry out an audit of the processing activities in the organisation.**	**Make the records of processing activities available on request to the Data Protection Office.**

Data Protection Impact Assessments

Data Protection Impact Assessments (DPIA)

What does the Act say?

*"Where processing operations are **likely to result in a high risk to the rights and freedoms of data subjects** by virtue of their nature, scope, context and purposes, every controller or processor shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."* ***(section 34 of the DPA)***

Data Protection Impact Assessments (DPIA)

What is high risk?

- Some examples of processing activities which is likely to result in high risk……. (but is not limited to):
  - where profiling operations are likely to significantly affect individuals;
  - where there is processing on a large scale of special categories of data, for instance a hospital processing its patients' genetic and health data across all its branches (hospital information system); or
  - where there is a systematic monitoring of a publicly accessible area on a large scale.

Data Protection Impact Assessments (DPIA)

What is high risk?

Case scenario

- a bank that screens its customers against a credit reference database; or
- a medical company offering genetic tests directly to consumers in order to assess and predict disease / health risks; or
- a new data processing technology is being introduced; or
- a company building behavioural or marketing profiles based on usage or navigation on its website.

Data Protection Impact Assessments (DPIA)

What does a DPIA address?

- **A DPIA can be useful for assessing multiple / single processing operations that are similar in terms of the risks presented,**
  - **provided adequate consideration is given to the specific nature, scope, context and purposes of the processing.**
- **For instance, where comparable technology is used to collect the same sort of data for the same purposes.**

Case scenario

- A transport operator may cover video surveillance systems in all its stations / buses / trains with a single DPIA.

Data Protection Impact Assessments (DPIA)

When a DPIA is not required?

- **Where the provisions under section 44 of the Data Protection Act are met**

Case scenario

- a medical doctor in a one-person practice may not be considered large scale; or
- a company organising a corporate event and needs to know what kind of food the invitees are allergic to, may not carry out a DPIA.

- **In cases where it is not clear whether a DPIA is required,**
  - **the Data Protection Office recommends that a DPIA is performed as it is a useful tool to help controllers or processors comply with data protection law.**

Data Protection Impact Assessments (DPIA)

Who is responsible for conducting a DPIA?

- ***Every controller or processor*** **must perform an assessment of the impact of the envisaged processing activities on personal data being safeguarded.**

Processing activities involving controllers & processors

- both need to define their respective obligations precisely;
- their DPIA must set out which party is responsible for the various measures designed to treat risks and to protect the rights & freedoms of individuals

Processing is wholly / partly performed by a processor

- the processor must assist the controller in carrying out the DPIA
- in certain circumstances, the view of individual may be sought

Data Protection Impact Assessments (DPIA)

When should we perform a DPIA?

- **A DPIA must be carried out prior to processing;**
- **DPIA incorporates the principles relating to processing of personal data by taking into consideration privacy by design principles;**
- **It also fosters projects to be compliant with privacy and data protection at the outset to avoid potential breaches.**

Case Scenario

- Building new IT systems for storing or accessing personal data; or
- Developing legislations / strategies that have privacy implications; or
- Embarking on a data sharing initiative.

Data Protection Impact Assessments (DPIA)

When should we review a DPIA?

- where organisational context for the processing activity has changed, such as:
  - personal data is intended to be transferred outside Mauritius and such data is likely to present high risks; or
  - effects of some automated decisions have become more significant; or
  - new categories of individuals become vulnerable to discrimination; or
  - personal data is being used for different purpose/s.
- when the context or components of processing operations evolve:
  - for instance the functionalities, purposes, risk sources, new vulnerabilities / threats may arise; or
  - there is a change of the risks presented by the processing operations.

Data Protection Impact Assessments (DPIA)

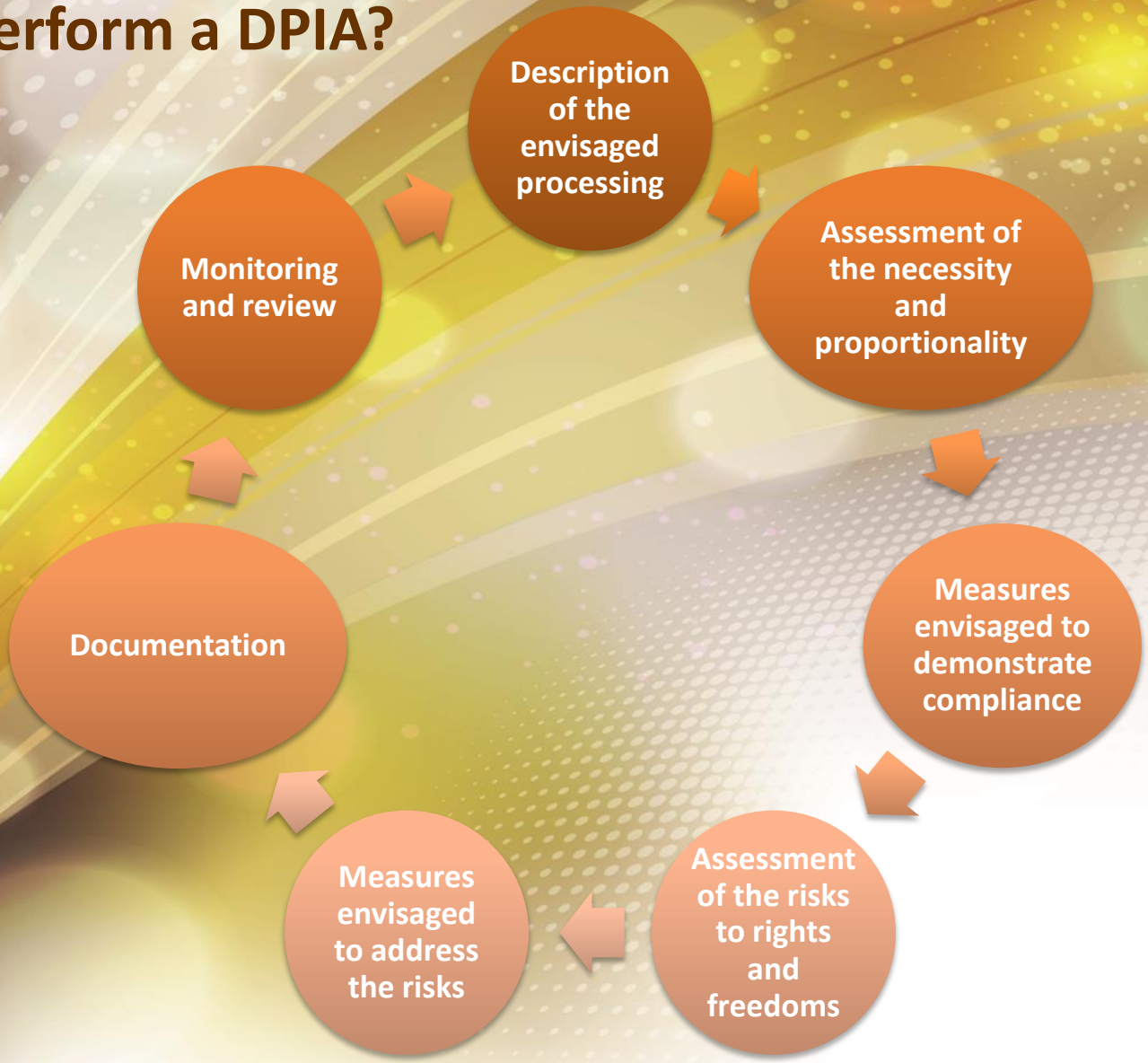
When should we review a DPIA?

- In general, it is a good practice to continuously perform a DPIA on existing processing activities.

- Nevertheless, depending on the nature of the processing as well as the rate of change in the processing operations or any other circumstances and the risks for the rights and freedoms are still mitigated:
  - a DPIA may be re-assessed after 3 years;
  - for instance the use of intelligent video analysis systems to automatically recognise license plates.

Data Protection Impact Assessments (DPIA)

How to perform a DPIA?



Data Protection Impact Assessments (DPIA)

Main Points & To do list

DPIA	Tool	Data Protection Office
A DPIA is required in situations where data processing is likely to result in high risks to individuals.	Familiarise yourself with the Privacy Compliance Assessment Web Application (PCA Web App) which is available on this office's website.	Publish a list of processing operations where DPIA will be mandatory and has designed a "Data Protection Impact Assessment Questionnaire" that can help controllers or processors .

Prior authorisation and Consultation

Prior authorisation and consultation

What does the Act say?

"Every controller or processor shall obtain authorisation from the Office prior to processing personal data ……. ……. in relation to the transfer of personal data to another country."
[Section 35(1) of the DPA]

"The controller or processor shall consult the Office prior to processing personal data……."
[Section 35(2) of the DPA]

Prior authorisation and consultation

Why authorisation and consultation is needed?

- Ensure compliance of the intended processing with the Act;

- Mitigate the risks involved for the individuals, where:
  - a controller or processor ***cannot provide for the appropriate safeguards*** referred to in section 36 *(in relation to the transfer of personal data to another country);*

  - processing operations, by virtue of their nature, scope or purposes, are likely to present a high risk:
    i. as indicated in section 34 (DPIA); or
    ii. this Office considers it necessary to carry out a prior consultation.

Prior authorisation and consultation

Why authorisation and consultation is needed?

- **Where this Office is of the opinion that the intended processing does not comply with the Act:**
  - ***in particular where risks are insufficiently identified or mitigated;***

- **this office shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.**

Prior authorisation and consultation

When authorisation and consultation must be sought?

Case Scenario

- *When processing health data on a large scale as it is considered as likely to result in a high risk.*

- **A list of the processing operations which are subject to prior consultation [as per section 33(2)(b)], shall be made public by the Data Protection Office**

Mrs Rushda Goburdhun
Data Protection Officer/Senior Data Protection Officer

Topics

- **Transfer of personal data outside Mauritius**
- **Rights of data subjects**
- **Unlawful disclosure of personal data**
- **Offences and Penalties**
- **Case studies**

What does the Act say about Transfer of personal data outside Mauritius?

Section 36 of the Act caters for transfer of personal data outside Mauritius.

- **Controller or processor has to provide to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data;**
- **Data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards;**
- **Section 36 (1) (c) provides other conditions where transfer can be made for example for the conclusion of contract, public interest requirements amongst others.**
- **Transfer is made from a register which according to law is intended to provide information to the public and which is open for consultation by public**

When should an organisation request authorisation from the Data Protection Commissioner?

No Safeguards

- *Where a controller or processor cannot provide for the appropriate safeguards in relation to the transfer of personal data to another country (Section 35(1)).*

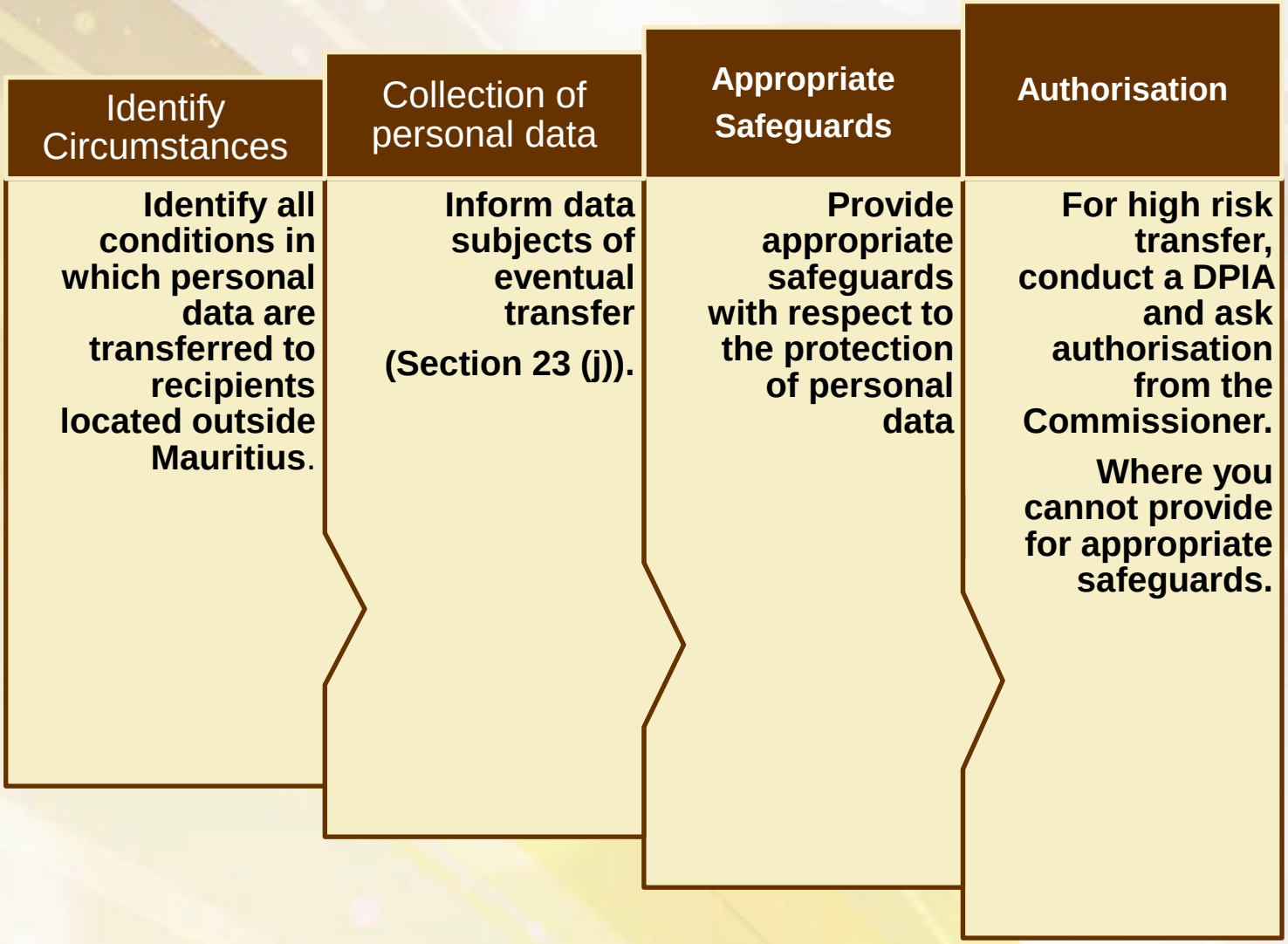
High Risk processing

- *Where the concerned transfer involves high risk to the rights and freedoms of the data subject.*

If consent has been provided by the data subject and it is necessary for the performance of a contract, can the organisation transfer data abroad in that case?

YES. If the organisation satisfies any one of the conditions laid down in section 36 then transfer of data outside Mauritius can be made.

Transfer of personal data outside Mauritius- TO DO

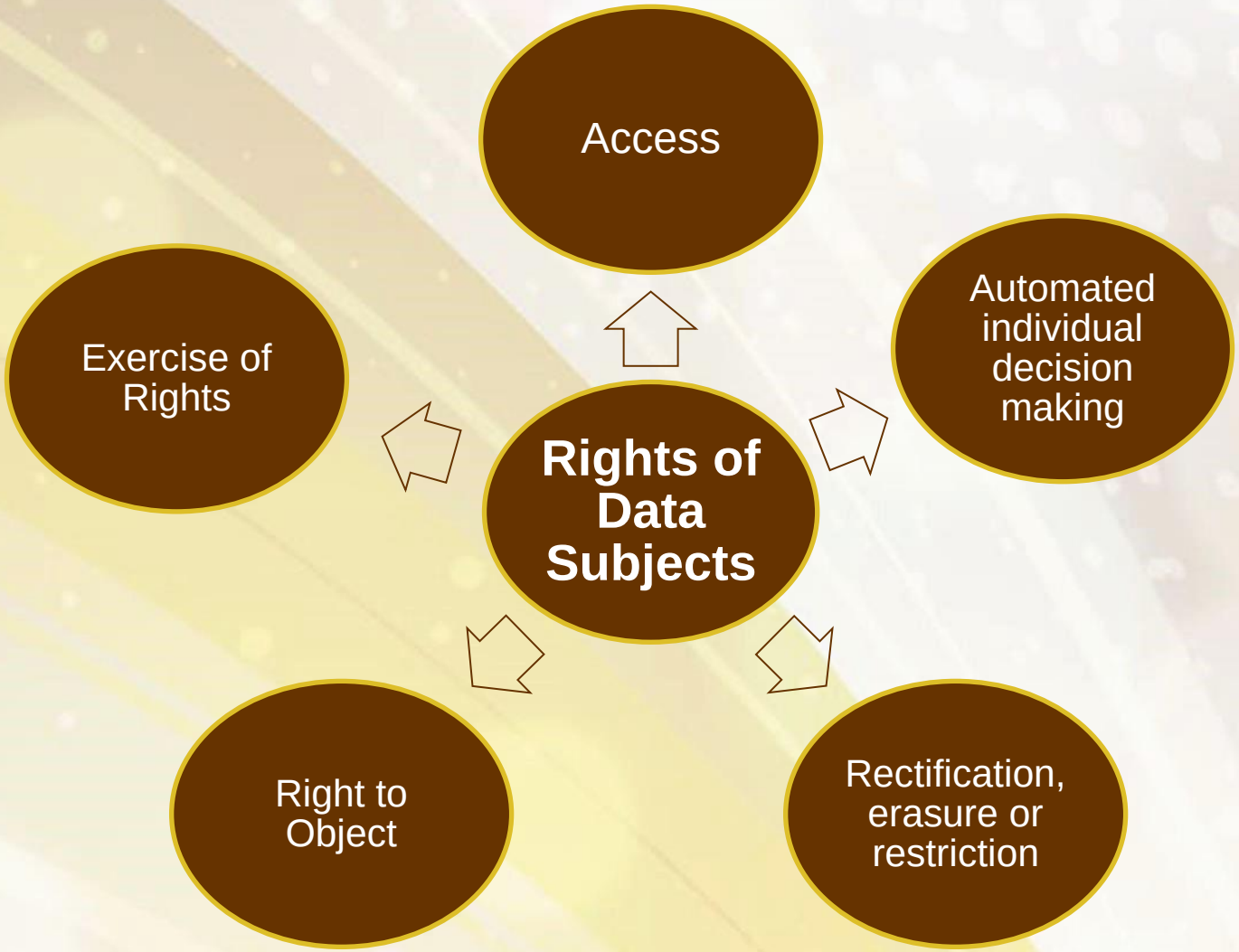


RIGHTS OF DATA SUBJECTS

Rights of Data Subjects

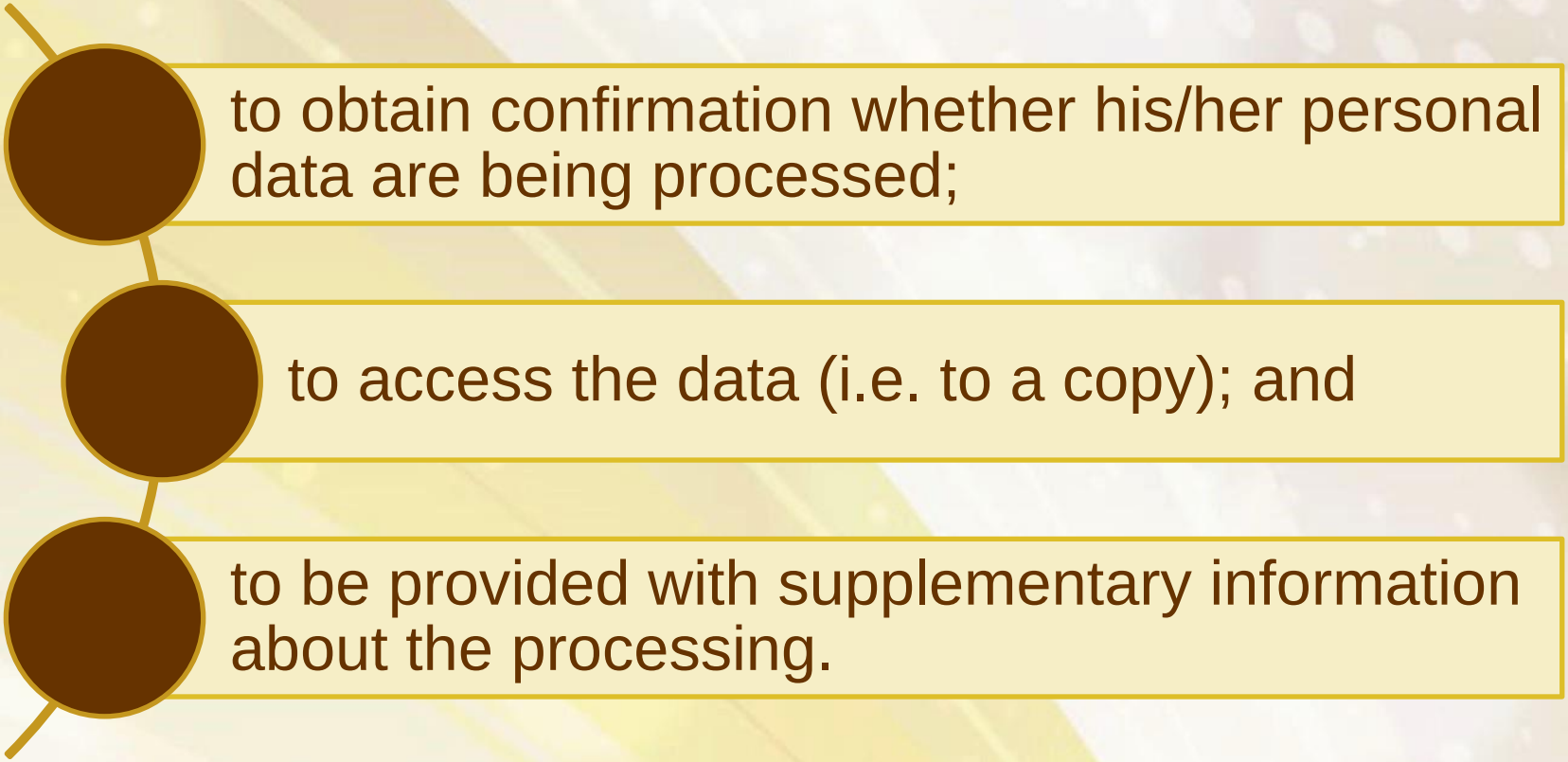
- **At a glance**
  - ✓ Part VII of the Act stipulates the rights of data subjects;
  - ✓ The Act has enhanced the rights to access, rectify, erase and restrict processing of personal data;
  - ✓ New provisions have been made to cater for decisions which are based on automated processing and the right to object to the processing of personal data by individuals.

Rights of Data Subjects



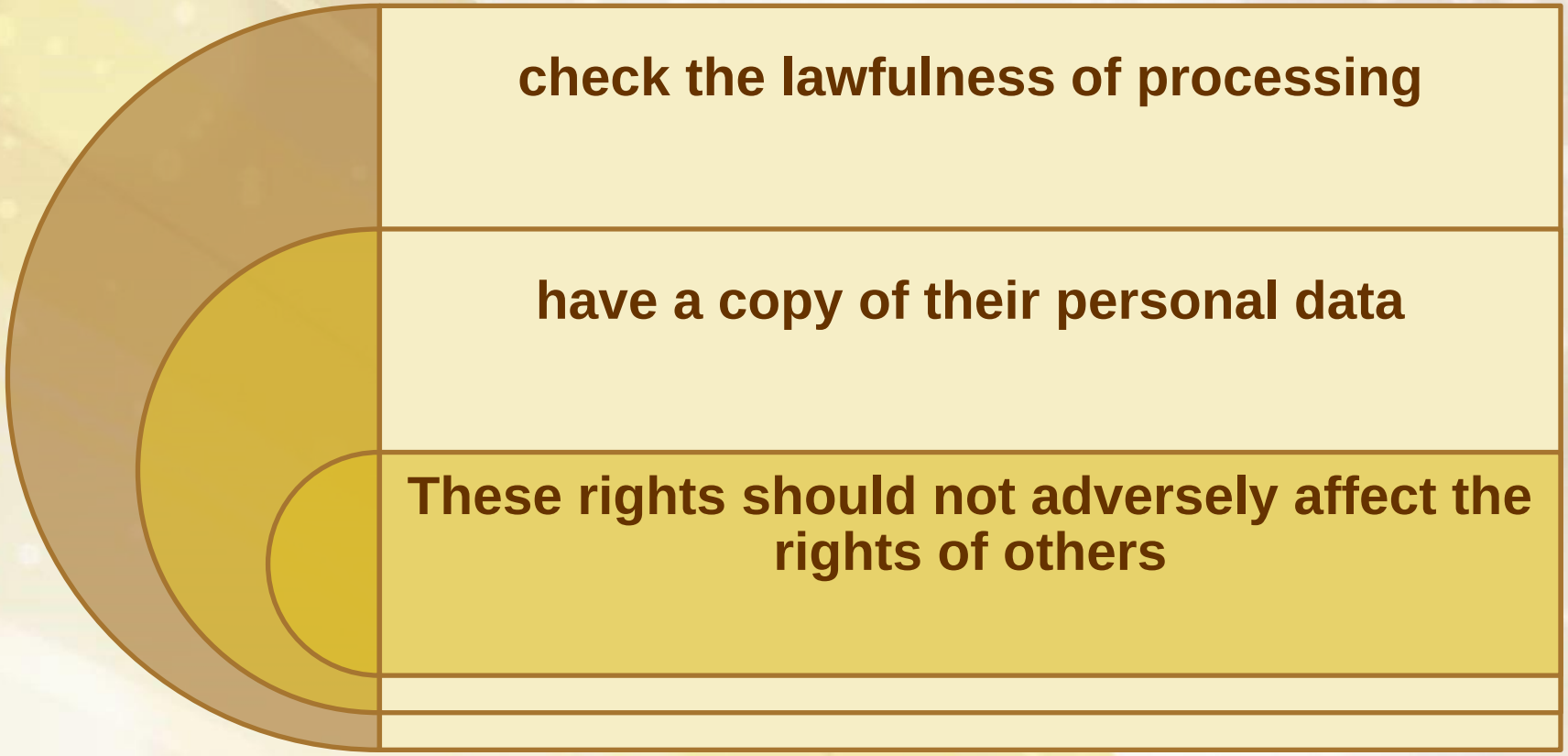
Rights of access (Section 37)

- ✓ An individual has the following rights:



Rights of access (Section 37)

Access rights are intended to allow individuals to:



Rights of access (Section 37)

- ✓ ***How to make a request of access?***
  - ❖ You should write to the controller or fill in the **Rights of Data Subject Form** available in the new Regulations.

- ✓ ***Can I charge a fee for dealing with a subject access request?***
  - ❖ You must provide a copy of the information **free of charge**.
  - ❖ However, where the request is manifestly excessive, you may charge a fee for providing the information or taking the action requested, or you may not take the action requested.

As a controller how should I handle an access request?

- Inform data subjects without undue delay and at latest within one month whether or not any action has been taken.
- If you refuse to take action on a request, inform the data subjects on the reason/s for the refusal and on the possibility of lodging a complaint with the Commissioner.
- If you have a reasonable doubt concerning the identity of a person making a request, you may request additional information to confirm the identity of the data subject.
- Information should be provided in an intelligible form, using clear and plain language.
- Examples of information to be provide as per section 37 (2) are: purpose of processing, categories of personal data, period of which data will be stored amongst others.

Automated individual decision making (Section 38)

- **In Brief**
  - ✓ The new Act makes provisions for the following:

automated individual decision-making

- Making a decision solely by automated means without any human involvement
- Example: Imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision- making process that does not necessarily involve profiling.

profiling

- automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.
- Examples of some fields where profiling is being carried out to aid decision making: Banking and finance, healthcare, taxation, insurance, marketing and advertising

Automated individual decision making (Section 38)

- ✓ Section 38 (1) says:

> ***The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or significantly affects him.***

- ✓ **When should a controller carry out an Automated individual decision making?**
  - ❖ it is necessary for the entry into or performance of a contract; or
  - ❖ It is authorised by law applicable to the controller; or
  - ❖ It is based on the individual's explicit consent.

Automated individual decision making (Section 38)

- ✓ **Transparency**
  - ❖ If you are making automated decisions as described in Section 38 (1) you must:
    - ➢ tell the data subject that you are engaging in this type of activity;
    - ➢ provide meaningful information about the logic involved; and
    - ➢ explain the significance and envisaged consequences of the processing.

- ✓ **Safeguards**
  - ❖ Implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Automated individual decision making (Section 38) – TO DO

Considered as high risk processing thus conduct a Data protection impact assessment to identify the risks to individuals.

You must identify and record your lawful basis for the processing.

You need to have processes in place for people to exercise their rights.

Individuals have a right to object to profiling in certain circumstances. You must bring details of this right specifically to their attention.

Secure personal data in a way that is in the interests and rights of the individual, and that prevents discriminatory effects.

Rectification, erasure or restriction of processing (Section 39)

- Data Subjects have the right to:

Rectify inaccurate or incomplete personal data

Delete or remove their personal data if the continued processing of those data is not justified

Withdraw their consent

Restrict the processing of their personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes)

Rights to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If controllers have disclosed the personal data in question to third parties, then they must inform them of the rectification where possible.

Controllers must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

Right to erasure

- Also known as '**right to be forgotten**'
- Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- the data are no longer needed for their original purpose (and no new lawful purpose exists);
- the data subject **withdraws consent**, and no other lawful ground exists;
- the data subject exercises the **right to object**, and the controller has no overriding grounds for continuing the processing;
- the data have been **processed unlawfully.**

When does the right to restriction of processing apply?

Where an individual **contests the accuracy** of the personal data, controller should restrict the processing until he or it has verified the accuracy of the personal data.

An individual has **objected to the processing** (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the controller is considering whether the organisation's legitimate grounds override those of the individual.

When processing is **unlawful** and the individual opposes erasure and requests restriction instead.

If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Right to Object (Section 40)

- What you need to know on right to object?

Data Subjects

- Data subjects have the right to object in writing, on grounds relating to their particular situation, to the processing of personal data.

Controllers

- Controllers must cease such processing unless they demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject; or requires the data in order to establish, exercise or defend legal rights.

As a controller, how do I comply with the right to object if I process personal data for direct marketing purposes?

- Stop processing personal data for direct marketing purposes as soon as you receive an objection
- Deal with the objection to processing for direct marketing at any time and free of charge. If necessary, review your procedures
- Inform individuals of their right to object “at the point of first communication“ and in your privacy notice

Exercise of rights (Section 41)

- *Where a person is a minor or physically or mentally unfit, a person duly authorised (parents, guardian, legal administrator) can exercise their rights on their behalf under this part.*

Unlawful disclosure of personal data

and

Offences and Penalties

Unlawful disclosure of personal data (Section 42)

Controller	Any controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected shall commit an offence.
Processor	Any processor who, without lawful excuse, discloses personal data processed by him without the prior authority of the controller on whose behalf the data are being or have been processed shall commit an offence

Offences and Penalties

- There are various offences and criminal penalties under this Act which, in general if committed, are sanctioned by a court of law.

- Where no specific penalty is provided, any person who does not comply or contravenes this Act shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

Offences and Penalties

For e.g.:

Offences	Penalties
Section 6: **Investigation of Complaints** Any person who fails to attend a hearing or to produce a document or other material when required to do so.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.
Section 7: **Power to require information** Any person who fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular.	Liable to a fine not exceeding 50, 000 rupees and to imprisonment for a term not exceeding 2 years.

Offences and Penalties

For e.g.:

Offences	Penalties
Section 15: Application for registration Any controller or processor who knowingly supplies any information, during registration, which is false or misleading in a material particular.	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.
Section 17: Change in particulars Any controller or processor who fails to notify a change in particulars.	Liable to a fine not exceeding 50, 000 rupees.
Section 28: Lawful processing Any person who process personal data unlawfully.	Liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years.

Case Studies

Case Study 1 : Can I have my daughter's records?

- Mrs B had concerns about her daughter Rosie's school performance and so made a request, on Rosie's behalf, for her education records. Rosie was aged eight and in grade three at primary school. The school asked for a fee of Rs 1000, which Mrs B paid. The school provided the records which consisted of 2 pages, 60 days later.

Case Study 1 (cntd)

1. **This case is about:**
   - access to education records; and
   - timescales and fees for subject access requests.

2. **What should be noted in this case?**
   - As per section 37 (5), the school should have provided a reply within one month from the date of request but instead took 60 days.
   - The information should have given free of charge since the information is manifestly not excessive (only 2 pages provided)

Case Study 2

- XYZ ltd is a company in the BPO sector. John Smith has been employed by the company since 3 years.
- The company usually stores salary details of all employees on its servers within its premises.
- One day, John came across one of these documents having the salary details of his colleagues.
- Later that evening, he opened the file at home and the next day he started to tell everyone about the salary of other colleagues.
- When the management came to know about this, he was dismissed with immediate effect and necessary measures were taken to secure the data.

Case Study 2 (cntd)

1. **Did John Smith commit a breach?**
   - Yes. John Smith unlawfully disclosed salary details of his colleagues as per section 42 of the DPA 2017.
2. **What about the XYZ Ltd?**
   - The company did not provide appropriate safeguards to protect the personal details of its employees and hence is in breach with section 31 of the DPA 2017 which is Security of Processing.
3. **Examples of measures that can be undertaken by XYZ Ltd to protect the salary details of its employees**
   - Password protect the file containing salary details of employees.
   - Restricted access to the confidential servers giving only the appropriate person access to these information.
4. **Should the company notify the Data Protection of that breach?**
   - Yes, this should be communicated as per section 25 of the DPA 2017.

Thank You

Mrs Warrda Khadun
Data Protection Officer/Senior Data Protection Officer

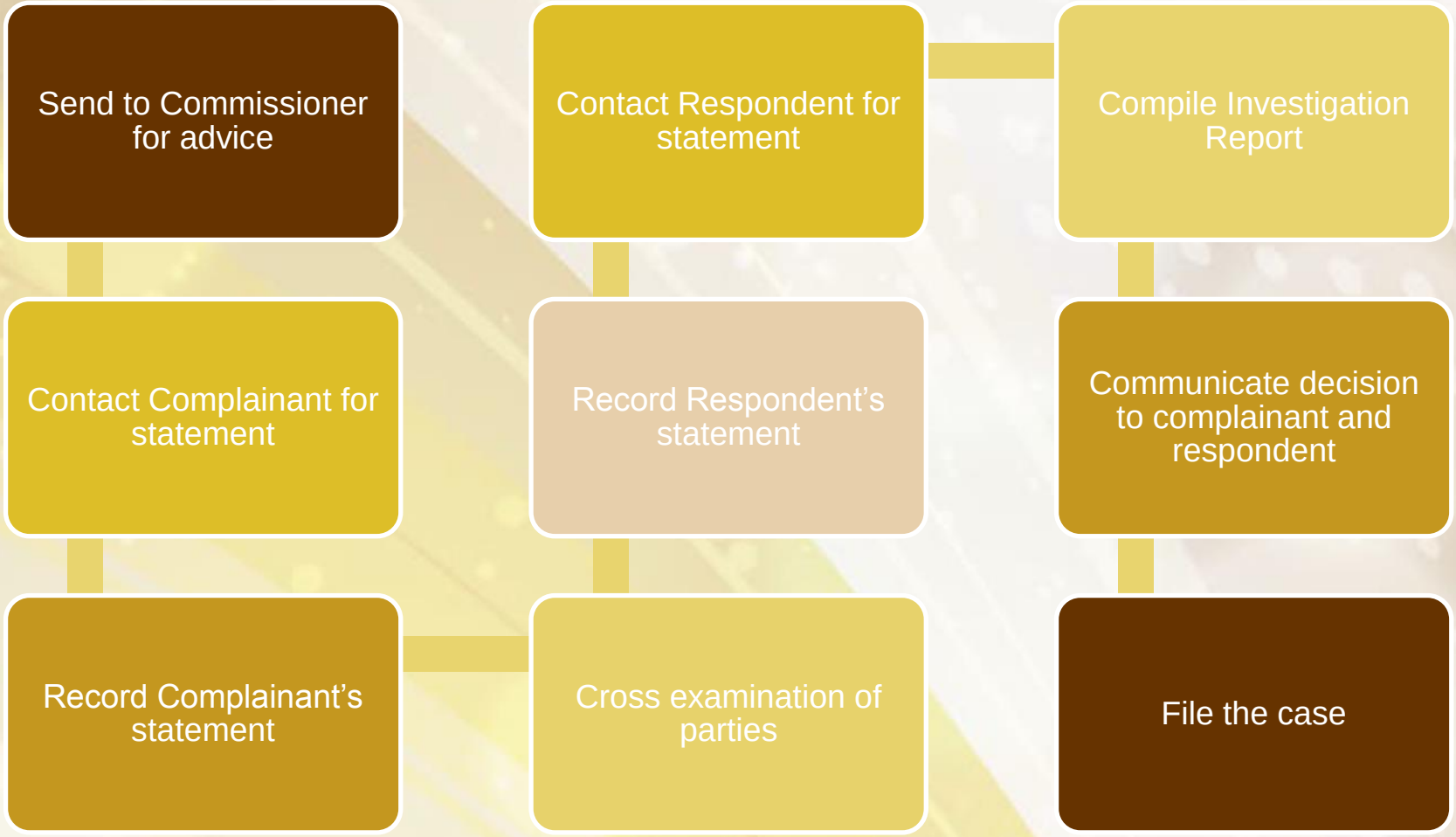
Topics

- **Investigation of complaints**
- **Exemptions and restrictions**
- **Certifications**

Investigation of complaints

- The Commissioner is empowered to investigate any complaint or information which gives rise to a suspicion that a offence may have been, is being or is about to be, committed under the DPA or cause it to be investigated by an authorised officer, unless he is of the opinion that the complaint is frivolous or vexatious .
- Investigation of complaints has always been part of the previous legislation but is now enhanced with the amicable resolution of disputes wherever possible.

How is the investigation carried out?



How long does the investigation take?

- Depending on the complexity of the cases, it may take 3 months to one year or more.

- It also depends on collaboration of all parties and availability/gathering of evidences.

What can be the outcome of the investigation?

An amicable resolution between the parties concerned

An offence being filed at the Office of the Director of Public Prosecution where the latter will decide if the offence has to be tried or not before a court.

Is the Decision of the Commissioner appealable?

- Yes, it is appealable at the ICT Appeal Tribunal set up under section 35 of the Information and Communication Technologies Act.

Case example 1

- **Unsolicited SMS messages**
  - **Mr X VS Shop Y**
    - **Mr X, a customer of shop Y accepted to receive messages about promotions from local shop Y.**
    - **Mr X started to receive messages from same brand shop of another country late at night and was unable to opt out.**
    - **Upon receiving the complaint, the office investigated and requested the shop to stop this practice and to provide customer with opt out facility.**
    - **Shop Y took necessary action to the satisfaction of the office and Mr X.**

Case example 2

- **Unlawful disclosure of personal data**
  - **Mr A VS Association B**
    - **Mr A, a member of association B lodged a complaint as his name was listed as outstanding debtor on the association B's website .**
    - **The office carried out an enquiry and found that and there was no specific law or regulation which requires association B to publish names of debtors online.**
    - **The association then removed the list of members with outstanding membership fees from its website.**

Exemptions and Restrictions

- Sections 3(4) and 44 depict the types of processing of personal data which are exempted from the DPA.

- The processing of personal data by an individual in the course of a purely personal or household activity is exempted from the DPA

Exemptions and Restrictions

- In general, processing of personal data constitutes a necessary and proportionate measure in a democratic society for the following reasons:

Exemptions and Restrictions

- The processing of personal data for the purpose of historical, statistical or scientific research is exempted provided that the security and organisational measures are implemented to protect the rights and freedoms of data subjects involved.

- The controller or processor has a duty to secure the data to prevent its unlawful disclosure. For instance, appropriate technology such as pseudonymisation or encryption can be used to secure the data.

Certification

- As per section 48 of the DPA, the Data Protection Office encourages the establishment of data protection certification mechanisms, seals and marks.

What is the purpose of certification?

- To enhance transparency and compliance with the Data Protection Act 2017, **certification (Section 48)** has been introduced to:
  - help controllers or processors to demonstrate accountability and compliance with the Act
  - build confidence and trust in the organisation with all stakeholders, as well as with the wider public
  - allow data subjects to quickly assess the level of data protection of relevant products and services
  - give legal certainty for cross-border data transfers

Certification

Certification body	• Certification will be issued by the Data Protection Office.
Compulsory and Fee?	• Certification is voluntary and free.
Validity	• Certification is valid for three years and is subject to renewal. Data controllers or processors may apply for renewal of the certification before the date of its expiry.
Withdrawal	• Certifications is subject to withdrawal where the conditions for issuing the certification are no longer met.

Does the absence of certification or failure in receiving certification have any negative effect on the controllers or processors?

- Having no certification does not mean that an organisation is less likely to be compliant.

- In addition, being unsuccessful in receiving a certification from the DPO or generally withdrawing from the certification application process is not sanctioned by the DPO, nor in itself carries negative inferences with respect to compliance.

How is the certification process carried out?

Apply
- Controllers or processors will need to apply for certification by filling in the application form.

Audit
- If registration and renewal payment is up to date, the data protection officers will conduct an audit on an arranged date at the controllers' or processors' premises.

Audit Report
- The data protection officers will write a report about their findings and will decide if certification can be granted.

Certification issued
- Certification with seal will be remitted to the controllers or processors.

Certification not issued
- Corrective actions will be recommended to the controllers or processors to be implemented in a number of days.

On the basis of which criteria is certification issued?

- Implementation of appropriate technical and organisational measures, including internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies
- Maintainance of relevant documentation on processing activities
- Implementation of measures that meet the principles of data protection e.g. data minimisation, pseudonymisation, improvement of security features on an ongoing basis
- Where appropriate, appointment of a data protection officer
- Use of data protection impact assessments where appropriate.

What are the benefits of certifications?

Certifications carry tangible benefits for individuals.

- Create trust
- Greater transparency
- Effective privacy protection

If implemented effectively, certifications may convey a number of key benefits to organisations

- Demonstrate accountability and compliance
- Enabling cross-border data transfers

Thank You

EMAIL: dpo@govmu.org