WORKSHOP ON
DATA PROTECTION ACT 2017

Hennessy Park Hotel
Presented by:
Mr V. Bhantoo
DPO / SDPO
15 May 2018
Agenda

1. Record of processing
2. Data Protection Impact Assessment (DPIA)
3. Prior authorisation & consultation
4. Transfer of personal data outside Mauritius
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
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’
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
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)*
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.
## Main Points & To do list

<table>
<thead>
<tr>
<th>Records</th>
<th>Audit</th>
<th>Data Protection Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keeping records of processing operation is compulsory.</td>
<td>Carry out an audit of the processing activities in the organisation.</td>
<td>Make the records of processing activities available on request to the Data Protection Office.</td>
</tr>
</tbody>
</table>
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)
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.
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.
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.
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.
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.
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?

1. Monitoring and review
2. Description of the envisaged processing
3. Assessment of the necessity and proportionality
4. Measures envisaged to demonstrate compliance
5. Measures envisaged to address the risks
6. Assessment of the risks to rights and freedoms
7. Documentation

Copyright © 2018 Data Protection Office. All rights reserved.
# Data Protection Impact Assessments (DPIA)

## Main Points & To do list

<table>
<thead>
<tr>
<th>DPIA</th>
<th>Tool</th>
<th>Data Protection Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>A DPIA is required in situations where data processing is likely to result in high risks to individuals.</td>
<td>Familiarise yourself with the Privacy Compliance Assessment Web Application (PCA Web App) which is available on this office’s website.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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]
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.
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.
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 35(2)(b)], shall be made public by the Data Protection Office.
TRANSFER OF PERSONAL DATA OUTSIDE MAURITIUS
What does the Act say?

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.
Transfer of personal data outside Mauritius

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 personal data outside Mauritius can be made.
## Transfer of personal data outside Mauritius

### Main Points & To do list

<table>
<thead>
<tr>
<th>Identify Circumstances</th>
<th>Collection of personal data</th>
<th>Appropriate Safeguards</th>
<th>Authorisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify all conditions in which personal data are transferred to recipients located outside Mauritius.</td>
<td>Inform data subjects of eventual transfer [Section 23(j)].</td>
<td>Provide appropriate safeguards with respect to the protection of personal data.</td>
<td>For high risk transfer, conduct a DPIA and ask authorisation from the Commissioner. Where you cannot provide for appropriate safeguards.</td>
</tr>
</tbody>
</table>
Thank You

Questions
CONTACT US

EMAIL : dpo@govmu.org
TEL : 460 0251
WEB : http://dataprotection.govmu.org