AN OVERVIEW OF THE DATA PROTECTION ACT 2017

Le Bocage International School

Presented by:
• Mrs J Haulkhory
• Mrs W Khadun

Hennessy Park, Ebene
21 June 2018
Agenda

- Aim of the Data Protection Act 2017 (DPA)
- Benefits of the Act
- The Data Protection Office
- Functions of the Data Protection Office (DPO)
- Definitions
- Registration
- Obligations on Controllers and Processors
- Processing operations likely to present risk
- Transfer of personal data
- Rights of Data Subjects
- Offences and penalties
- Certification
Aim of the DPA

Came into force on 15 January 2018

To strengthen the control and personal autonomy of data subjects (individuals) over their personal data

In line with the European Union’s General Data Protection Regulation (GDPR)

To simplify the regulatory environment for business in our digital economy.

To promote the safe transfer of personal data to and from foreign jurisdictions
Benefits of the Act

- Increased accountability of controllers
  - Implement better processes
  - Better Organisation
  - Better Productivity
  - Strengthen customer trust
  - Gain confidence and trust

- Enhanced data subjects’ rights of individuals for greater control over their personal data.

- Improve the digital legal landscape to respond to the new EU requirements for adequacy, thereby attracting foreign investors.

- Minimised risk of data breaches
The Data Protection Office

• Public office which acts with complete independence and impartiality.

• Not subject to the control or direction of any other person or authority in the discharge of its functions

• Head of the Office is the Data Protection Commissioner.
Functions of DPO

I. Ensure compliance with the DPA 2017 and regulations

II. Registration of controllers and processors

III. Investigation of complaints

IV. Sensitisation/ training

V. Exercise control on all data protection issues

VI. Conduct data protection compliance audits

VII. Cooperate with other supervisory authorities

VIII. Research on data processing and computer technology
• DEFINITIONS
Data Subject

• An identified or identifiable individual
• In particular by reference to an identifier such as a name, ID, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity
Personal Data

Any information relating to a data subject:

- Names of staff and pupils
- Dates of birth
- Addresses
- National insurance numbers
- Assessments data
- School marks
- Exam results
- Staff development reviews
Other Definitions

Processing
- Operations performed on personal data, including automated means.
- For e.g collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination

Controller
- A person who or public body which, alone or jointly with others
- Determines the purposes and means of the processing of personal data
- Has decision making power with respect to the processing

Processor
- A person who, or a public body which, processes personal data on behalf of a controller
• REGISTRATION
Registration

“... no person shall act as controller or processor unless he or it is registered with the Commissioner...”, Part III, Section 14

• Validity of Registration Certificate: 3 years

• Renewal: 3 months prior to expiry

• Notification of change in particulars within 14 days

• Cancellation or variation of terms of Registration Certificate.
• OBLIGATIONS OF PROCESSORS AND CONTROLLERS
## Obligations on Controllers & Processors

Implement appropriate technical and organisational measures for compliance

<table>
<thead>
<tr>
<th>Collection of personal data for lawful purpose(s)</th>
<th>Bear the burden of proof for consent prior to processing</th>
<th>Notify and communicate personal data breach</th>
<th>Ensure appropriate data security and organisational measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duty to destroy personal data</td>
<td>Ensure lawfulness of processing of personal data</td>
<td>Keep record of all processing operations</td>
<td>Comply with requirements to process special category of data</td>
</tr>
<tr>
<td>Consent for processing personal data for children</td>
<td>Perform a data protection impact assessment</td>
<td>Comply with req. of prior authorisation or consultation from DPO</td>
<td>Designate a data protection officer</td>
</tr>
</tbody>
</table>
Details to be provided to data subjects:

- Contact details of the controller/processor and the representative
- Purpose(s) for which the school holds personal data
- To whom they intend to disclose the data.
- Whether the collection is voluntary or mandatory
- Period for storing the data
- Right to withdraw consent at any time
- Rights of data subjects: Access, Rectification, Erasure, Object to Processing
- To which countries they intend to transfer the data.
- Automated decision making, and the consequences of such processing.
- Right to lodge a complaint with the Commissioner
Principles relating to processing of personal data

Lawfulness, Fairness, Transparency

Explicit, Specified, Legitimate Purpose(s)

Adequate, Relevant, Limited to what is necessary

Accurate, Up-to-date

Storage Limitation – Data Subjects identified for no longer than necessary

In accordance with the rights of the data subjects
Collection of information (about a child, parent or staff member) must be clear and transparent about the purpose(s).

Clear explanation about reason for processing personal data (for example: to facilitate education or to arrange school trips).

Need for privacy notice with:

- what information is needed
- why it is being collected
- which third parties it may be passed on to.

Consent is required for the data processed

- Including whether you are sharing data between people or online, such as photographs on the school’s Facebook page
Privacy Notices

Possible use of Privacy Notices:

- In any enrolment documentation
- On the bottom of any forms used to collect personal information
- In the school reception area or on the school’s website

May indicate mandatory data fields at the time of collection to make it clear to the person what they must fill in and where they can leave spaces blank.

Information must not be collected just because it might become useful later – it must be essential for the present intended purpose.
To Do’s for Fair Processing

Request parents and students to check that their details are correct on a periodic basis.

Correct any inaccurate data.

Any personal data that is out of date or no longer needed must be ‘destroyed’.

Must specify the retention period of records before disposal.
Schools must not acquire data and process it in any manner that doesn’t relate to the intended purpose.

For example: data acquired about students for assessments can’t then be used on the school’s website.

Determining what may be excessive includes looking at forms and deciding what information is absolutely critical for the intended purpose.

Anything else may be considered excessive and irrelevant.
Lawful processing

No person shall process personal data unless the data subject consents to the processing for one or more specified purposes

Or

exceptions apply (for example)

for the performance of a contract to which the data subject is a party

for compliance with any legal obligation to which the controller is subject

to protect the vital interests, amongst others
Conditions for consent

- Consent must be freely given, specific, informed and unambiguous.
- Consent must be able verifiable.
- Consent can be withdrawn at any time.
Special categories of personal data

Personal data relating to: for e.g

- physical or mental health, racial or ethnic origin, political opinion,
- religious or philosophical beliefs, physical or mental health or condition

Now includes “genetic data” and “biometric data”.

Merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.
## Personal data of a child

- Children have the same rights as adults over their personal data.

- Children merit specific protection with regard to their personal data.

- Children are less aware of the risks, consequences and safeguards and their rights in relation to the processing of personal data.

- Parental consent for children under the age of 16.

- “Reasonable efforts” by the controller to verify consent.
Personal data of a child

To have a lawful basis for processing a child’s personal data and to decide the basis before processing:

To rely upon consent, a need to ensure that personal data is erased when the individual gave his consent to processing when he was a child.

To rely upon performance of a contract, to consider the child’s competence to agree to the contract and to understand the implications of this processing.

To rely upon legitimate interests, to balance your own legitimate interests in processing the personal data against the interests and fundamental rights and freedoms of the child.
Notification & Communication of personal data breach

Notify the personal data breach to the Commissioner without undue delay

Where feasible, not later than 72 hours of becoming aware of the breach

The controller must communicate that breach to the data subject

For e.g An officer has disclosed personal details of parents to a marketing company.
Duty to destroy personal data

Where the purpose for keeping personal data has lapsed,

Every controller shall destroy the data as soon as is reasonably practicable; and

Notify any processor holding the data, who must destroy the data specified by the controller as soon as is reasonably practicable.

For e.g Need to delete emergency number of parents for students who have already left the school.
Security of processing

Appropriate technical and organisational measures must be implemented to prevent unauthorised access to, alteration, disclosure, accidental loss and destruction of personal data.

Such measures include:

- Pseudonymisation and encryption of personal data
- Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems
- Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident
- Process for regularly testing, assessing, and evaluating the effectiveness of TOMs
If the controller is using the services of a processor, the controller is still responsible under the DPA for data protection and so must ensure through a written contract that the processor acts only on instructions received from the controller and implements appropriate security measures for protecting any personal data processed.

The Data Protection Commissioner may carry out inspection and assessment of the security measures imposed on the controller or processor.
Records of processing operations

The new Act requires the controller and processor to keep records of processing activities under its responsibility.

Such records must include:

- Name and contact details of controller or processor or any representative
- Purpose of processing
- Description of categories of data subjects and personal data
- Description of categories of recipients
- Details of transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules
- Description of technical and organisational security measures.

These records must be made available, on request, to the Data Protection Office.
• PROCESSING OPERATIONS LIKELY TO PRESENT RISKS
A DPIA is a process to help you identify and mitigate the data protection risks of a project.

**DPIA is mandatory when the processing is likely to result in a high risk for the rights and freedom of individuals, including some specified types of processing such as:**

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people
- Process special category data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
Data Protection Impact Assessment (DPIA)

DPIA must:

- describe the nature, scope, context and purposes of the processing;
- check that the processing is necessary for and proportionate to the purposes;
- identify and assess risks to individuals (by considering their likelihood and severity); and
- identify any measures to address (eliminate or reduce) those risks.
According to Section 35, the controller or processor must seek authorisation and consult the Data Protection Office prior to processing personal data in order to ensure compliance of the intended processing with the DPA and in particular to mitigate the risks involved for data subjects (individuals) where the controller or processor cannot provide for the appropriate safeguards required for the transfer of personal data to another country.
• TRANSFER OF PERSONAL DATA
As per section 36(1) of the Data Protection Act 2017 (DPA), a controller or a processor may transfer personal data to another country where –

- Proof of appropriate safeguards
- Consent from data subject
- Contract with data subject
- Public interest
- Legal claim
- Vital interest
- Legitimate interest
• RIGHTS OF DATA SUBJECTS
Rights of Data Subjects

Right of access

- A data subject has the right to obtain confirmation that his/her personal data is processed and a copy of the data free of charge within one month following a written request.

Automated individual decision making

- A data subject has the right not to be subject to a measure which is based on profiling by means of automated processing.

Rectification

- A data subject has the right to obtain from controller rectification of inaccurate or incomplete personal data concerning him/her.
Rights of Data Subjects

**Erasure**
- Data subject may request that his/her personal data are erased if the continued processing of those data is not justified.

**Restriction of processing**
- A data subject may request that the processing of his/her personal data is restricted where the accuracy of the data is contested.

**Right to object**
- A data subject has the right to object in writing at any time the processing of personal data relating to him/her free of charge.
• Where a person is a minor or a physically or mentally unfit, a person duly authorised (parent, guardian, legal administrator) can exercise his/her rights under the DPA.
Unlawful disclosure of personal data

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.

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
Offences and Penalties

There are various offences and criminal penalties under the DPA 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 the Act shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.
• CERTIFICATION
Certification

• To enhance transparency and compliance with the DPA, certification 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

- The Data Protection Office encourages the establishment of data protection certification mechanisms, seals and marks.

<table>
<thead>
<tr>
<th>Certification body</th>
<th>• Certification will be issued by the Data Protection Office.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compulsory and Fee?</td>
<td>• Certification is voluntary and free.</td>
</tr>
<tr>
<td>Validity</td>
<td>• Certification is valid for three years and is subject to renewal.</td>
</tr>
<tr>
<td>Withdrawal</td>
<td>• Certifications is subject to withdrawal where the conditions for issuing the certification are no longer met.</td>
</tr>
</tbody>
</table>
Contact Us:

Website: [http://dataprotection.govmu.org](http://dataprotection.govmu.org)

Email: dpo@govmu.org

Tel: 460 0251