



**The Ministry of Technology, Communication and
Innovation
and
The Data Protection Office**

**Workshop On
DATA PROTECTION ACT 2017**

**Tuesday 06 March 2018
from 08.30 hrs – 15.30 hrs**

**InterContinental Mauritius Resort,
Balaclava Fort, Coastal Road,
Balaclava**



Topics

- **Registration**
- **Principles relating to Processing of personal data**
- **Roles and Responsibilities of Controllers**
- **Roles of Data Protection Officer**

Mrs Jasbir B. HAULKHORY
Data Protection Officer/Senior Data Protection Officer

Registration

Part III, Section 14

Why to Register?

“... no person shall act as controller or processor unless he or it is registered with the Commissioner...”



Part III, Section 14: Legal Requirement to Register

Who should Register?

Medical Practitioner, Barrister, Ministry,
private companies

Controller

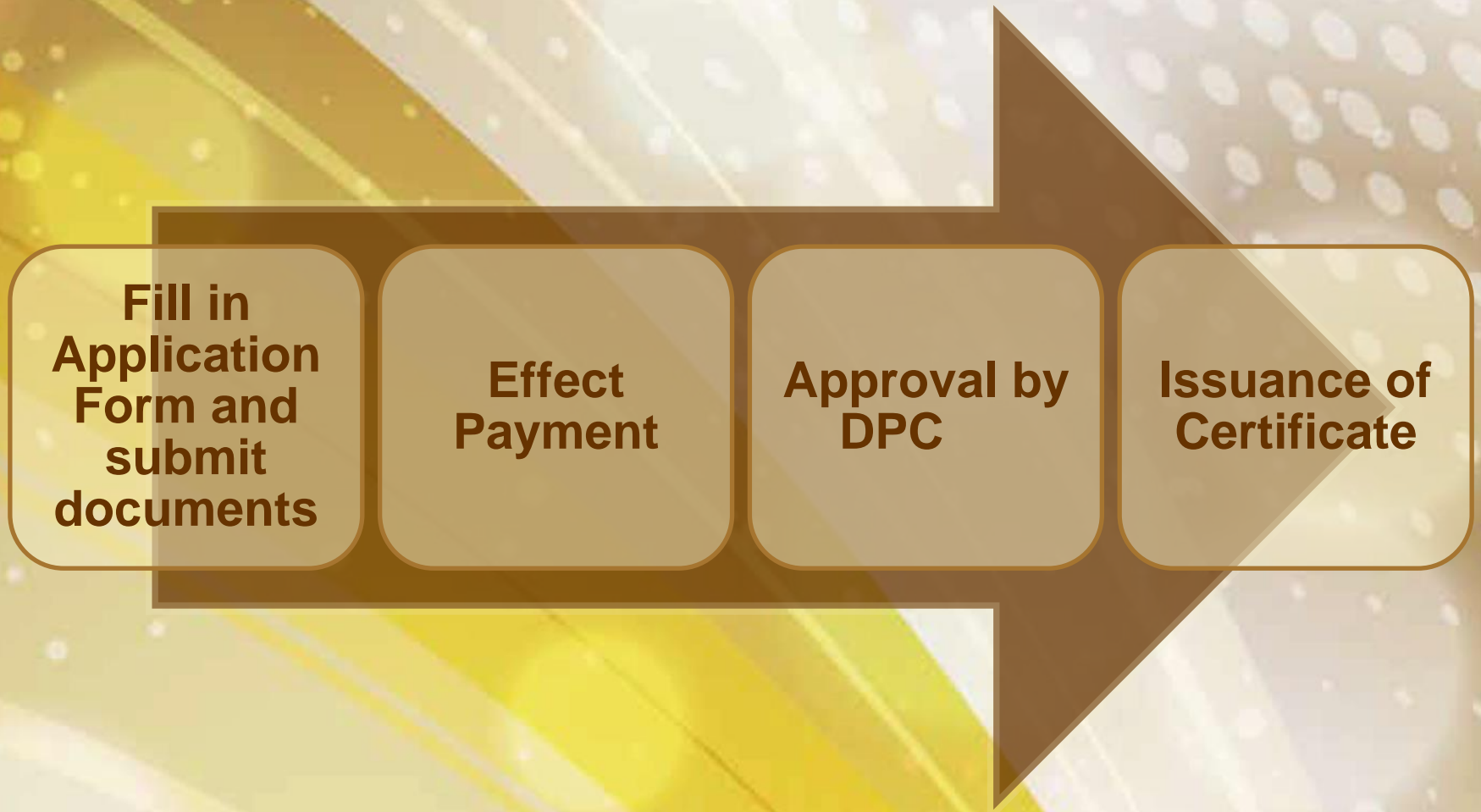
- A person who or public body which, alone or jointly with others,
 - determines the purposes and
 - means of the processing of personal data and
 - has decision making power with respect to the processing.

Company A manages and hosts servers of Company X

Processor

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

Process of Registration



Registration Form



Amendment to Registration / Renewal

With the coming of the New
Regulation

● Only 1 form for Registration and amended fee structure

● Validity of Registration Certificate: 3 Years

● Renewal Deadline: 3 months prior to Expiry Date

● Notify the Commissioner about the change in particulars within 14 days

● Cancellation and variation of Terms of Registration Certificate

Offence

For providing any false or misleading information in the particulars of information

A fine not exceeding 100,000 rupees

Imprisonment for a term not exceeding 5 years

Offence

**Failure to notify about
change in particulars**

**A fine not exceeding
50,000 rupees**

6 Privacy Principles for Controllers and Processors

Principles relating to Processing of Personal Data

Section 21

Principles relating to Processing of personal data (1)

Lawfulness, fairness and transparency

- *Employer to disclose salary details of employees to tax authorities, without consent.*

Purpose limitation

Explicit, specified and legitimate purposes and not processed in a way incompatible with the purposes

- *A General Practitioner cannot disclose patients details to his wife who owns a travel agency.*

Data minimisation

Adequate, relevant and limited to what is necessary, in relation to the purposes

- *Specific questions about health conditions are queried to only relevant manual occupations.*

Principles relating to Processing of personal data (2)

Accuracy:

Accurate and, where necessary, up-to-date. Erasure and rectification without delay.

- *A mis-diagnosis of a medical condition is still kept as it is relevant for the treatment given to the patient or to additional health problems.*

Storage limitation:

Storage of personal data permitting identification of data subjects for no longer than necessary

- *Deletion of emergency numbers for staff who have left the organisation.*

Data subjects' rights:

Processing in accordance with data subject's rights

- *Rectification of an incorrect address*

TO-DO List

Review internal policies and audit procedures

Update these policies and procedures where necessary to ensure that they are consistent with the revised principles.

Provide appropriate training to ensure that the business is thinking about data protection issues at all levels.

Roles and Responsibilities of Controllers

Part IV

Roles and Responsibilities of Controllers/Processors (1)



Roles and Responsibilities of Controllers/Processors(2)

Collection of data for a lawful purpose and is necessary for that purpose

Bear the burden of proof for data subject's consent for the processing of personal data

Notify and Communicate about for Personal Data Breach

Ensure appropriate data security and organisational measures

Duty to destroy personal data as soon as purpose lapses

Ensure the lawfulness of processing of personal data

Comply with the requirements to process Special Category of Personal Data

Consent for the processing of personal data of children

Keep records of all processing operations under his or its responsibility

Perform data protection impact assessment for high risks operations

Comply with the requirements for prior authorisation or consultation from DPO

Designate an officer responsible for data protection compliance issues

Collection of Personal Data

Section 23



For a lawful purpose connected with a function or activity of the controller



Necessary for that purpose

Collection of Personal Data

Direct or Indirect Collection – Requirement to inform data subjects about:

Identity and Contact details of the controller and its representative

Purpose of the personal data

Intended Recipients of the data

Whether the collection is voluntary or mandatory

Existence of the right to withdraw consent at any time

Existence of right of rectification, restriction, erasure of personal data and to object to processing

Existence of Automated decision making, and the consequences of such processing

Period for storing personal data

Right to lodge a complaint with the Commissioner

Transfer of personal data abroad and the adequacy of protection by that country

Further information necessary to guarantee fair processing of the personal data

Exemption

Indirect Data Collection

- The data subject already has the information.
- The provision of such information proves impossible or would involve a disproportionate effort.
- The recording or disclosure of the data is laid down by law.

Role of Data Protection Officer

Section 22

Who can be a Data Protection Officer?

Mandatory appointment of an officer responsible for data protection compliance issues.

Professional with experience and knowledge of data protection laws

Existing Employee

As long as there is no conflict of interest with professional duties

New Employee

External Officer

As long as there is a rigorous contract for appropriate safeguards

Roles of Data Protection Officer

Inform and advise the controller/processor and the employees about the obligations to comply with the DPA 2017

Monitor compliance with the DPA 2017

Advise on data protection impact assessments

Train staff

Conduct internal audits

Be the point of contact for the Data Protection Office and for individuals whose data are processed

Obligations of Controllers/Processors

**Determine
whether to
appoint a Data
Protection
Officer**

**Enable DPO
to work
Independently**

**Ensure that
DPO reports
to the highest
management**

**Provide
adequate
resources to
fulfill the
obligations
under the DPA
2017**

Thank you

WORKSHOP ON DATA PROTECTION ACT 2017

The background of the central section is a blurred image of a lightbulb, with the bulb itself in sharp focus in the foreground. The background is a mix of blue and white light streaks, suggesting motion or a bright environment.

The Secret of Getting Ahead Is Getting Started

Mark Twain

Date: 06 March 2018

Venue: Intercontinental Hotel, Balaclava Fort



AGENDA



Consent

Notification of personal data breach and Communication of personal data breach to data subject

By Mrs Pravina Dodah

Data Protection Officer/Senior Data Protection Officer



**What is
consent?**

Consent

Indication signifying agreement to processing

Freely Given

Specific

Informed



Unambiguous by statement or a clear affirmative action

Elements of valid consent

Freely given	Provide genuine choice Not penalised for refusing consent
Specific	Concise on the processing operation and purpose/s.
Informed	Provide clear information and in plain language , at minimum containing: <ul style="list-style-type: none">• The controller's identity,• The purpose/s of the processing,• The processing activities,• The right to withdraw consent at any time Amount of information depends on circumstances and context of a case
Unambiguous indication (by statement or a clear affirmative action)	To avoid implied form of actions by the data subject such as pre-ticked opt-in boxes



**How is consent
in DPA 2017
different from
DPA 2004 ?**

Differences

Definition

**Unambiguous
by statement
or a clear
affirmative
action**

Conditions

Controllers have the burden of proof for establishing consent

Data subject can withdraw his consent anytime

Consent is presumed not to be freely given if the performance of a contract, including the provision of a service, is dependent on the consent which is not necessary for such execution of the contract/service.

Suppose a customer has a contract with a bank for ordinary bank account services. In the contract, the bank asks customers consent to use their payment details for marketing and customer's refusal would lead to the denial of banking services.



**Why should
consent matter
to me?**

Is one
criterion to
demonstrate
that you are
processing
data lawfully

28. Lawful processing

- (1) No person shall process personal data unless –
 - (a) the data subject consents to the processing for one or more specified purposes;
 - (b) the processing is necessary –
 - (i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
 - (ii) for compliance with any legal obligation to which the controller is subject;
 - (iii) in order to protect the vital interests of the data subject or another person;
 - (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (v) the performance of any task carried out by a public authority;

When is consent not appropriate?

Other lawful criteria for processing where consent is not appropriate:

- A contract with the individual**
- Compliance with a legal obligation**
- Vital interests**
- Tasks carried by public authority / public interest**
- Legitimate interests unless outweighed by harm to the individual's rights and interests**
- Historical, statistical or scientific research**

Example:

A company sells goods online. A customer purchases a refrigerator and has a contract with the company where he has to provide his address for delivery of the refrigerator.

The processing of address by the company is necessary for the service, i.e., purchase and covered under ‘for performance of a contract to which the data subject is party’.

When is consent not appropriate?

- If you would still process the personal data without consent, asking for consent is misleading.

Example

A financial institution provides credit facilities to its customers and asks them to give consent for their personal data to be sent to MCIB (Mauritius Credit Information Bureau).

However, if a customer refuses or withdraws his consent, the company will still send the data to MCIB on the basis of 'for compliance with any legal obligation to which the controller is subject'.

When is consent not appropriate?

- If you make 'consent' a precondition of a service which goes beyond the execution of the service, consent is unlikely to be the most appropriate lawful basis.

Example: A mobile app for photo editing asks its users to have their GPS activated for the use of its services.

Since users cannot use the app without consenting to GPS, the consent is unlikely to be appropriate.

To do list



Make an assessment whether consent is the appropriate lawful ground for the envisaged processing.

Ensure consent is valid.

Implement simple and easy-to-access ways to withdraw consent.

Keep evidence of consent – who, when, how, and what you told people.

AGENDA



Consent

Notification of personal data breach and Communication of personal data breach to data subject



**What is a
personal data
breach?**

Personal data breach

“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”

Examples

A person gains access to a controller’s customer database and discloses the information to an unauthorised person.

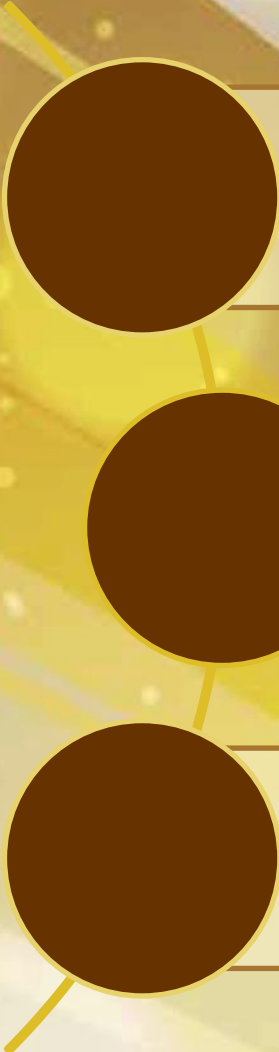
A controller is hit by a Denial of Service attack causing disruption to the normal service and unavailability of personal data.

An attacker modifies the database of credit information held by a company.



When does a controller/processor becomes “aware” of a personal data breach ?

When do you become aware?



Associated to a point where the controller has a reasonable degree of certainty that a breach has occurred

Clear or quick preliminary investigation required

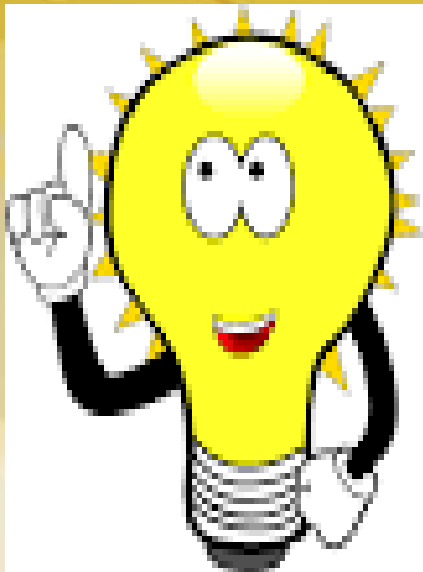
Take prompt action to investigate whether a breach has occurred or not

Example

A controller suspects that his network has been accessed by an intruder. He quickly verifies and finds that his data has been compromised.



What should a processor do?



Notify the controller without any undue delay as soon as the processor becomes aware of the personal data breach.



**What should a
controller do?**

Timing



1

Notify the Data Protection Commissioner

Without undue delay and where feasible not later than 72 hours after being aware of it

2

Communicate the personal data breach to the data subject **where it is likely to result in a high risk to the rights and freedoms of the data subject**

Without undue delay after notifying the Data Protection Commissioner



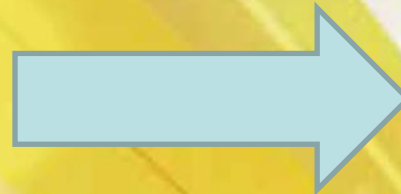
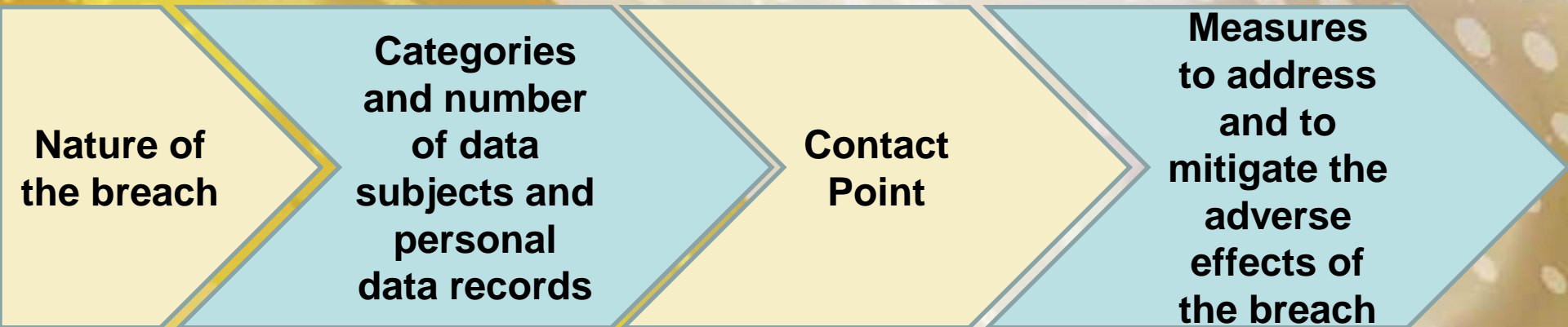
What happens if I cannot meet the timing delay of 72 hours to report to the Data Protection Commissioner?



Reasons for delay have to be provided to the Data Protection Commissioner

How to report a personal data breach?

Personal Data Breach Notification Form



**DATA
PROTECTION
OFFICE**

Are there circumstances where communication to data subjects is NOT required?


- Appropriate security measures were already applied before the breach such as encryption which rendered the data unintelligible;**
- The controller has taken subsequent measures to ensure that the breach is unlikely to result in a high risk to the rights and freedoms of the data subjects.**
- It would involve disproportionate effort and the controller has made a public communication or similar measure whereby a data subject is informed in an equally effective manner.**

To do list

Make sure you have appropriate technical and organisational protection measures to protect data.




Determine whether to set up a breach response team.




To regularly review and update all procedures for addressing breaches.



Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.



Determine whether any other external third party/ies need to be notified to limit the potential impact.



Thank You

WORKSHOP ON DATA PROTECTION ACT 2017

TOPICS:

**Lawful Processing,
Personal data of children and
Security of processing.**

By Mr R. Mukoon

Data Protection Officer/Senior Data Protection Officer

Date: 06 March 2018

Venue: Intercontinental Hotel, Balaclava Fort

Lawful Processing S28

Consent

- The data subject consents to the processing for one or more specified purposes

Example

- A Marketing Company building a marketing database for a campaign

Lawful Processing S28

Contract

- For the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering a contract

Example

- You made an online purchase, the controller processes your address in order to deliver the goods. This is necessary in order to perform the contract.

Lawful Processing S28

Contract

- For the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering a contract

Example

- You will enter into a life insurance contract. The controller requires some medical test of you before entering into the contract. This is necessary prior to entering into the life insurance contract.

Lawful Processing S28

Legal Obligations

- The controller is subject to comply with some legal obligations

Example

- An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to MRA.

Example

- A court order may require you to process personal data for a particular purpose and this also qualifies as a legal obligation.

Lawful Processing S28

Vital Interests

- In order to protect the **vital interests** of the data subject or another person

Example

- An individual is admitted to the ICU department of a hospital and that person is unable to communicate to doctors . The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests.

Lawful Processing S28

Official Authority
Vested

- For the performance of a task carried out in the public interest **or in the exercise of official authority vested in the controller**

Example

- The National Pension department requires your identity card details for processing pension given to you. Here the controller can show that he is exercising official authority and no additional public interest test is required.

Lawful Processing S28

Legitimate
Interests pursued
by controller

- For the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject

... 3 part tests

1. Purpose test: are you pursuing a legitimate interest?
2. Necessity test: is the processing necessary for that purpose?
3. Balancing test: do the individual's interests override the legitimate interest?

Lawful Processing S28

Legitimate Interests
Example

- The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.

*... Direct
Marketing example*

- The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

Lawful Processing S28

Marketing to do lists

Automation

- Consider implementing an automated system that can be used to log and monitor consent and contact preferences. This should be made available to anyone who needs to make contact with individuals so that checks can be made prior to contact to ensure contact is permitted.

Procedures
and
processes

- Updating procedures and processes to ensure they meet the DPA 2017 requirements to embed practices across the organisation. This will mean that your compliant processes will be effortless and will be business as usual..

Train your
teams

- Another area where organisations will need to dedicate time and resource to is training and awareness to ensure that all employees are conscious of their responsibilities as well as the changes that the DPA 2017 has brought.

Lawful Processing S28

Historical ,
Statistical or
Scientific Research

- For the purpose of historical, statistical or scientific research . Security and organizational measures have to be implemented to protect the rights and freedoms of data subjects involved.

Example

- Health data for scientific research needs to be anonymized
- Statistical results are normally published as aggregate data
- Historical data is necessary for the particular controller.

Children Under DPA 2017

Consent by
Parent or
Guardian

- No person shall process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian.

Example

- Primary and secondary schools are directly concerned. They must ensure that consent received are carefully documented. Issuing a receipt to a minor, controller must ensure that the receipt is issued to the parent or guardian rather than the child under 16.

Children Under DPA 2017

Reasonable effort for consent

- Where the personal data of a child below the age of 16 years is involved, a controller shall make every reasonable effort to verify that consent has been given or authorised, taking into account available technology.

Example

- If the data processing is targeting children and depend on children's consent, then the processing organization need to consider following two requirements.
 - 1.Implements age-verification mechanism.
 - 2.Verify parental responsibility

Children Under DPA 2017

Age
Verification
mechanism

- **Controller can rely on the verification against official documents or school card issued to students or verification of potential child data against the population database.**

*Child
Personal
Data*

- **Personal data of child has same rights as adults under the Data Protection Act 2017.**
- **Ensure that verification are carefully carried out before processing child personal data.**

Children Under DPA 2017

Age Verification
mechanism

- “...the practice of leveraging electronic identities as their preferred method of age verification for the following reasons: it provides a reliable, fast, convenient, proportionate approach to age verification that enables operational efficiencies, lower levels of both fraud and identity theft, higher levels of customer satisfaction, convenience, and more effective self-regulatory measures ...”
Source:<https://www.oii.ox.ac.uk/archive/downloads/publications/Effective-Age-Verification-Techniques.pdf>

Child Personal
Data

- Personal data of child has same rights as adults under the Data Protection Act 2017.
- Ensure that verification are carefully carried out before processing child personal data.

Security of Processing S31

Appropriate security
and organizational
measures

- A controller or processor shall, at the time of the determination of the means for processing and at the time of the processing implement *appropriate security and organisational measures* for the prevention of unauthorised access to, the alteration of; the disclosure of; the accidental loss of; and the destruction of, the data in his control.

Confidentiality

- Confidentiality is the ability to hide information from those people unauthorised to view it. It is perhaps the most obvious aspect of the CIA triad when it comes to security;
- It is also the one which is attacked most often. Cryptography and Encryption methods are an example of an attempt to ensure confidentiality of data transferred from one computer to another.

Security of Processing S31

Pseudonymisation

- means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

...

- The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Act is not intended to preclude any other measures of data protection.

Security of Processing S31

Integrity

- The ability to ensure that data is an accurate and unchanged representation of the original secure information.
- One type of security attack is to intercept some important data and make changes to it before sending it on to the intended receiver.

Availability

- It is important to ensure that the information concerned is readily accessible to the authorised viewer at all times.
- Some types of security attack attempt to deny access to the appropriate user, either for the sake of inconveniencing them, or because there is some secondary effect. For example, by breaking the web site for a particular organisation, a rival may become more popular.

Security of Processing S31

Security controls ISO27002:2013

Security policy

- Policies for information security
- Review of the policies for information security

Organization of information security

- Internal Organization
- Information security roles and responsibilities
- Segregation of duties
- Contact with authorities
- Contact with special interest groups
- Information Security in Project Management

Mobile Devices

- Mobile device policy
- Teleworking

Human Resources Security

- Prior to employment screening
- Terms and conditions of employment
- Management responsibilities
- Information security awareness, education and training
- Disciplinary process
- Termination or change of employment responsibilities

Security of Processing S31

Security Controls ISO27002:2013

Asset Management

- Responsibility for Assets
- Inventory of Assets
- Ownership of assets
- Acceptable use of assets
- Information classification
- Classification guidelines
- Labelling of information
- Handling of assets
- Media handling
- Management of removeable media
- Disposal of media
- Physical Media transfer

Access Control

- Business requirements for access control
- Access control policy
- Access to networks and network services
- User access management
- User registration and deregistration
- User access provisioning
- Management of privileged access rights
- Management of secret authentication information of users
- Review of user access rights
- Removal or adjustment of access rights

User responsibilities

- Use of secret authentication information
- Application and information access control
- Information access restriction
- Sensitive system isolation
- Password management system
- Use of privileged utility programs
- Access control to program source code

Human Resources Security

- Prior to employment
- Screening
- Terms and conditions of employment
- During employment
- Management responsibilities
- Information security awareness, education and training
- Disciplinary process
- Termination or change of employment
- Termination or change of employment responsibilities

Security of Processing S31

Security controls ISO27002:2013

Asset Management

- Responsibility for Assets
- Inventory of Assets
- Ownership of assets
- Acceptable use of assets
- Information classification
- Classification guidelines
- Labelling of information
- Handling of assets
- Media handling
- Management of removable media
- Disposal of media
- Physical Media transfer

Access Control

- Business requirements for access control
- Access control policy
- Access to networks and network services
- User access management
- User registration and deregistration
- User access provisioning
- Management of privileged access rights
- Management of secret authentication information of users
- Review of user access rights
- Removal or adjustment of access rights

User Responsibilities

- Use of secret authentication information
- Application and information access control
- Information access restriction
- Sensitive system isolation
- Password management system
- Use of privileged utility programs
- Access control to program source code

Human Resources Security

- Prior to employment
- Screening
- Terms and conditions of employment
- During employment
- Management responsibilities
- Information security awareness, education and training
- Disciplinary process
- Termination or change of employment
- Termination or change of employment responsibilities

Security of Processing S31

Security controls ISO27002:2013

Equipment security

- Equipment siting and protection
- Supporting utilities
- Cabling Security
- Security of equipment off-premises
- Equipment maintenance
- Removal of assets
- Security of equipment and assets off-premises
- Secure disposal or re-use of equipment
- Unattended user equipment
- Clear desk and clear screen policy

Operations Security

- Operational procedures and responsibilities
- Documented operating procedures
- Change management
- Capacity management
- Separation of development, testing and operational environments
- Protection against malicious and mobile code
- Controls against malicious code
- Backup
- Information Backup
- Logging and monitoring
- Event logging
- Protection of log information
- Administrator and operator logs
- Clock synchronisation

Control of operational software

- Installation of software on operational systems
- Technical Vulnerability Management
- Management of technical vulnerabilities
- Restrictions on software installation
- Information Systems audit considerations
- Information systems audit controls

Communications Security

- Network security management
- Network controls
- Security of network services
- Segregation in networks
- Information transfer
- Information transfer policies and procedures
- Agreements on information transfer
- Electronic messaging
- Confidentiality or non-disclosure agreements

Systems acquisition, development and maintenance

- Information security requirements analysis and specification
- Securing application services on public networks
- Protecting application services transactions
- Security in development and support processes
- Secure development policy
- System change control procedures
- Technical review of applications after operating platform changes
- Restrictions on changes to software packages
- Secure system engineering principles
- Secure development environment
- Outsourced software development
- System security testing
- System acceptance testing
- Test data
- Protection of test data

Security of Processing S31

Security controls ISO27002:2013

Supplier relationships

- Information security in supplier relationships
- Information security policy for supplier relationships
- Addressing security within supplier agreements
- Information and communication technology supply chain
- Supplier service delivery management
- Monitoring and review of supplier services
- Managing changes to supplier services

Information security incident management

- Reporting information security events and weaknesses
- Responsibilities and procedures
- Reporting information security events
- Reporting information security weaknesses
- Assessment of and decision on information security events
- Response in information security incidents
- Learning from information security incidents
- Collection of evidence

Information security aspects of business continuity management

- Information security continuity
- Planning information security continuity
- Implementing information security continuity
- Verify, review and evaluate information security continuity
- Redundancies
- Availability of information processing facilities

Compliance

- Compliance with legal and contractual requirements
- Identification of applicable legislation
- Intellectual Property Rights (IPR)
- Protection of records
- Privacy and protection of personally identifiable information
- Regulation of cryptographic controls
- Information security reviews
- Independent review of information security
- Compliance with security policies and standards
- Technical compliance review

Security of Processing S31

Standards

- The Office may lay down technical standards for the requirements in section 31 (1) of the Act.

Transmission of data over an information and communication network

- In determining the appropriate security measures referred to in subsection (1), in particular, where the processing involves the transmission of data over an information and communication network, a controller shall have regard to –
 - (a) the state of technological development available;
 - (b) the cost of implementing any of the security measures;
 - (c) the special risks that exist in the processing of the data; and
 - (d) the nature of the data being processed.

Security of Processing S31

Contract

- Where a controller is using the services of a processor –
- (a) he or it shall choose a processor providing sufficient guarantees in respect of security and organisational measures for the purpose of complying with subsection (1); and
- (b) the controller and the processor shall enter into a written contract which shall provide that –
- (i) the processor shall act only on instructions received from the controller; and
- (ii) the processor shall be bound by obligations devolving on the controller under subsection(1).

Security of Processing S31

Employee
awareness
of security

- Every controller or processor shall take all reasonable steps to ensure that any person employed by him or it is aware of, and complies with, the relevant security measures. For example training on Phishing

Lawful Processing, Personal data of Children and Security of processing

Thank You