WORKSHOP ON DATA PROTECTION ACT 2017

TOPICS:
Consent,
Lawful Processing,
and
Security of processing.

By Mr R. Mukoon
Data Protection Officer/Senior Data Protection Officer

Date: 15 May 2018
Hennessy Park Hotel
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

<table>
<thead>
<tr>
<th>Freely given</th>
<th>Provide genuine choice and control for data subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not penalised for refusing consent</td>
</tr>
<tr>
<td>Specific</td>
<td>Concise on the processing operation and purpose/s.</td>
</tr>
<tr>
<td>Informed</td>
<td>Provide clear information and in plain language, at minimum containing:</td>
</tr>
<tr>
<td></td>
<td>• The controller’s identity,</td>
</tr>
<tr>
<td></td>
<td>• The purpose/s of the processing,</td>
</tr>
<tr>
<td></td>
<td>• The processing activities,</td>
</tr>
<tr>
<td></td>
<td>• The right to withdraw consent at any time</td>
</tr>
<tr>
<td></td>
<td>Amount of information depends on circumstances and context of a case</td>
</tr>
<tr>
<td>Unambiguous indication (by statement or a clear affirmative action)</td>
<td>To avoid implied form of actions by the data subject such as pre-ticked opt-in boxes</td>
</tr>
</tbody>
</table>
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.
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.
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**
- Open a bank account: all necessary personal data required for the processing of a bank account is lawful processing.
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

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

- 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

- 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.

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

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

- 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

- 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.

- 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.

- 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

- 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.
Security of Processing S31

- 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 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 website 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 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

<table>
<thead>
<tr>
<th>Asset Management</th>
<th>Access Control</th>
<th>User Responsibilities</th>
<th>Human Resources Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Responsibility for Assets</td>
<td>• Business requirements for access control</td>
<td>• Use of secret authentication information</td>
<td>• Prior to employment</td>
</tr>
<tr>
<td>• Inventory of Assets</td>
<td>• Access control policy</td>
<td>• Application and information access control</td>
<td>• Screening</td>
</tr>
<tr>
<td>• Ownership of assets</td>
<td>• Access to networks and network services</td>
<td>• Information access restriction</td>
<td>• Terms and conditions of employment</td>
</tr>
<tr>
<td>• Acceptable use of assets</td>
<td>• User access management</td>
<td>• Sensitive system isolation</td>
<td>• During employment</td>
</tr>
<tr>
<td>• Information classification</td>
<td>• User registration and deregistration</td>
<td>• Password management system</td>
<td>• Management responsibilities</td>
</tr>
<tr>
<td>• Classification guidelines</td>
<td>• User access provisioning</td>
<td>• Use of privileged utility programs</td>
<td>• Information security awareness, education and training</td>
</tr>
<tr>
<td>• Labelling of information</td>
<td>• Management of privileged access rights</td>
<td>• Access control to program source code</td>
<td>• Disciplinary process</td>
</tr>
<tr>
<td>• Handling of assets</td>
<td>• Management of secret authentication information of users</td>
<td></td>
<td>• Termination or change of employment</td>
</tr>
<tr>
<td>• Media handling</td>
<td>• Review of user access rights</td>
<td></td>
<td>• Termination or change of employment responsibilities</td>
</tr>
<tr>
<td>• Management of removable media</td>
<td>• Removal or adjustment of access rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Disposal of media</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Physical Media transfer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Equipment security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Equipment siting and protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Supporting utilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Cabling Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Security of equipment off-premises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Equipment maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Removal of assets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Security of equipment and assets off-premises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Secure disposal or re-use of equipment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Unattended user equipment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Clear desk and clear screen policy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

**Communication 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

<table>
<thead>
<tr>
<th>Supplier relationships</th>
<th>Information security incident management</th>
<th>Information security aspects of business continuity management</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Information security in supplier relationships</td>
<td>• Reporting information security events and weaknesses</td>
<td>• Information security continuity</td>
<td>• Compliance with legal and contractual requirements</td>
</tr>
<tr>
<td>• Information security policy for supplier relationships</td>
<td>• Responsibilities and procedures</td>
<td>• Planning information security continuity</td>
<td>• Identification of applicable legislation</td>
</tr>
<tr>
<td>• Addressing security within supplier agreements</td>
<td>• Reporting information security events</td>
<td>• Implementing information security continuity</td>
<td>• Intellectual Property Rights (IPR)</td>
</tr>
<tr>
<td>• Information and communication technology supply chain</td>
<td>• Reporting information security weaknesses</td>
<td>• Verify, review and evaluate information security continuity</td>
<td>• Protection of records</td>
</tr>
<tr>
<td>• Supplier service delivery management</td>
<td>• Assessment of and decision on information security events</td>
<td>• Redundancies</td>
<td>• Privacy and protection of personally identifiable information</td>
</tr>
<tr>
<td>• Monitoring and review of supplier services</td>
<td>• Response in information security incidents</td>
<td>• Availability of information processing facilities</td>
<td>• Regulation of cryptographic controls</td>
</tr>
<tr>
<td>• Managing changes to supplier services</td>
<td>• Learning from information security incidents</td>
<td></td>
<td>• Information security reviews</td>
</tr>
<tr>
<td></td>
<td>• Collection of evidence</td>
<td></td>
<td>• Independent review of information security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Compliance with security policies and standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Technical compliance review</td>
</tr>
</tbody>
</table>
Security of Processing S31

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

- 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(6)

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.
Consent, Lawful Processing, and Security of processing

Thank You