Data Protection Challenges The New EU GDPR

Drudeisha Madhub, Data Protection Commissioner

13 October 2017

Overview

- Aim of the proposed amendments
- Key definitions in the GDPR
- Data Protection Commission
- Obligations of Controllers
- Data Protection Register
- Rights of Data Subjects
- Miscellaneous
- Benefits of new proposed law
- Q&A

Aim of the proposed amendments

- To align our existing Data Protection Act (DPA) with

  - current technological and other advancements that have occurred since our DPA was enacted in 2004 and

  - relevant international standards namely the New EU General Data Protection Regulation 2016/679 (commonly known as the GDPR) and the European Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (commonly known as Convention 108).

Key definitions in GDPR

- Data Controller

  the person 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 such processing

- Data Subject

  an identified or identifiable natural person in particular by reference to an identifier such as name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- Personal data

  means any information relating to a data subject

Data Protection Commission

- Data Protection Commission

  The Data Protection Commission must be able to exercise its functions with complete independence, adequate resources and enforcement powers to impose sanctions since these are essential components of the right to protection of personal data as duly recognised by the European Court of Human rights and the European Court of justice in their jurisprudence in compliance with international standards.

- Powers of the Commissioner

  The Commissioner must have enhanced powers with regard to handling of complaints namely the amicable resolution of disputes whenever possible and the streamlining of existing procedures.

Obligations of Controllers

- Responsibility of Controller

  The controller must ensure all personal data is processed in compliance with the Act, and be able to demonstrate compliance through a series of measures including keeping of documentation, designating a data protection officer, among others.

- Notification of a personal data breach to the Commission

  As soon as the controller becomes aware that a breach has occurred, the controller must notify the breach to the Commission.

- Communication of a personal data breach to the data subject

  The controller must also communicate the personal data breach to the data subject without undue delay unless the breach is unlikely to result in a high risk.

Obligations of Controllers

- Records of processing operations

  The controller are required to keep extensive and detailed records of processing activities and to make those records available, on request, to the Commission.

- Data protection impact assessment

  A data protection impact assessment must be carried out by the controller prior to any potentially high risk processing.

- Prior authorisation and prior consultation

  Where the controller does not provide for the appropriate safeguards for the transfer of personal data to another country, the controller must obtain authorisation from the Commission before processing. Moreover, where a data protection impact assessment indicates that processing operations involve high risks, the controller must consult the Commission prior to processing.

Obligations of Controllers

- Certification

  The establishment of certification mechanisms, data protection seals and marks will provide a means for data controllers to demonstrate compliance thereby allowing data subjects to quickly assess the level of data protection of relevant products and services.

- Collection of personal data

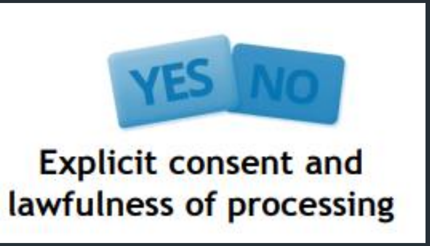
  The principles of fair and transparent processing require the controller to provide information about itself, the purposes of processing and explain to data subjects how their personal data will be processed (e.g. existence of automated decision-making including profiling), the consequences of such processing and their individual rights (e.g. existence of the right to withdraw consent).

Obligations of Controllers

- Processing of special categories of personal data
  - “Special categories of personal data” (presently known as sensitive personal data under the DPA) now expressly include “genetic data” and “biometric data” where processed “to uniquely identify a person”.
  - The grounds for processing sensitive data under the GDPR broadly replicate those under the existing DPA, although there are wider grounds in the area of health and healthcare management.
    - A number of exceptions to the restrictions on processing health data, including where the processing is necessary for various medical assessments and where the processing is necessary for reasons of public interest in public health.

Obligations of Controllers

- Consent
  - Consent must be freely given, specific, informed and unambiguous.
  - The controller must be able to supply evidence that consent has been obtained(verifiable).
  - Consent can be withdrawn at any time.



- Processing of personal data of a child
  - Children are “vulnerable individuals” deserving “specific protection”.
  - Parental consent must be obtained for children under the age of 16.
  - The controller is also required to make “reasonable efforts” to verify that consent has been given by the holder of parental responsibility in light of available technology

Obligations of Controllers

- Data Security
  - Enhanced obligations in comparison to current legislation.
  - In addition to security measures for ensuring confidentiality, integrity, availability and recovery from failure, introduction of new requirements such as pseudonymisation and encryption.

- Transfer of personal data outside Mauritius

  Transfer of personal data to another country may take place only if the controller has adduced appropriate safeguards with respect to the protection of personal data to the Commission or has complied with the conditions laid down in the provisions of this Act relating to the transfer of personal data outside Mauritius.

Rights of Data Subjects

- Right of access (faster response time and free)

  Every data subject will have the right, where personal data are processed, to obtain free of charge a copy of the data concerning him/her within one month following a written request .

- Automated individual decision-making, including profiling
  - Every individual will have the right not to be subject to a measure which is based on profiling by means of automated processing.
  - However, such measure will be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent.
  - In any case, such processing will have to be subject to suitable safeguards.

Rights of Data Subjects

- Right to rectification, restriction of processing and/or erasure
  - Any person will have the right to obtain from controller rectification of inaccurate or incomplete personal data concerning him/her.
  - Data subjects may request that their personal data are erased where
    - the data are no longer necessary for the purposes for which the data are collected,
    - the data subjects have withdrawn their consent for processing,
    - the data subjects object to the processing of personal data,
    - the processing of their personal data is unlawful.
  - Restriction provides an alternative to erasure and gives a temporary solution where the accuracy of the data is contested or the processing on grounds argued as legitimate by the controller is objected and such accuracy or legitimate basis for processing cannot be immediately proven.

Rights of Data Subjects

- Right to object
  - The data subject will have the right to object in writing at any time the processing of personal data relating to him/her free of charge. E.g. processing is pursuant to the controller's legitimate interests or for purposes of direct marketing
  - The burden of proof will be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.

Miscellaneous

- Exceptions and restrictions
  - The current exceptions and restrictions are being simplified to promote legal certainty such that no exception to the provisions set out in the GDPR will be allowed except when provided by law and when it constitutes a necessary and proportionate measure in a democratic society.
  - However, a data subject or the Commission may apply for a judge's order whenever the exception is deemed illegal.
- Right of appeal

  Each individual will have the right to a judicial remedy against decisions of the Commission concerning them. Proceedings against the Commission will be brought directly before the Supreme Court.

Benefits of new proposed law

- Increased accountability of data controllers will make organisations implement controlled business processes resulting in better organisation, greater productivity and efficiency, and higher level of security.
  - Being compliant will also help organisations to gain and strengthen customer trust, confidence and loyalty.
- Enhanced data subjects' rights will give individuals greater control over their personal data.
- The risk of data breaches will be minimised.
- The legal and practical certainty for economic operators and public authorities will be reinforced.
- The new data protection framework will significantly improve the digital legal landscape to respond to the new EU requirements for adequacy, thereby attracting foreign investors.

Questions