

The proposed General Data Protection Regulation

The Institute of Operational Risk

3 December 2013

Melanie Shillito, Director, Promontory
mshillito@promontory.com

Agenda

- I. Background
- II. Progress/Next Steps
- III. The proposed General Data Protection Regulation (GDPR)
 - i. Territorial Scope
 - ii. New Definitions
 - iii. Principles and Processing Conditions
 - iv. Information Policies
 - v. Information to the Individual
 - vi. Individuals' Rights
 - vii. Data Controller/Processor Obligations
 - viii. Data Protection Officer
 - ix. Certification
 - x. Personal Data Transfers to Third Countries
 - xi. Sanctions

Background

- Current Data Protection legislation stems from EU Directive 95/46/EC
- Not all EU Member States implemented the Directive the same way
- The UK is seen as being pragmatic and business friendly, many other countries as requiring too much red tape
- The proposed General Data Protection Regulation was published in January 2012
- The Committee of the European Parliament responsible for reviewing the European Commission proposals is the Committee on Civil Liberties, Justice and Home Affairs ('LIBE')

Progress/Next steps

- In January 2013 the Rapporteur presented his draft report to the LIBE Committee
 - The report included detailed changes after consultation with various stakeholders
 - The changes would increase the burdens on organisations
- Other Committees and interested parties tabled in the region of 4,000 amendments
- Difficult for LIBE to consider and incorporate suggested amendments into revised text for vote by Parliament
- LIBE vote was postponed several times but finally took place on 21 October - their proposed compromise agreement was passed
- The Plenary Vote is set for 14 April
- May 2014 deadline may be too difficult to achieve – decision will be made this week

Colour Key

Text in black = original Commission proposal

Text in red = proposal to remove under the Compromise Agreement

Text in blue = proposal to include under the Compromise Agreement

Territorial Scope

- The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU.
- The GDPR applies to processing of personal data relating to individuals residing in the EU by controllers established outside of the EU where activities relate to:
 - The offering of goods and services; or
 - The monitoring of individuals **their behaviour**
- If the controller is established outside of the EU, and the above provision applies, a representative in the EU must be appointed unless:
 - The controller is established in an EU ‘approved country’
 - Goods and services are offered only occasionally
 - The enterprise employs less than 25 people
 - The controller is a public authority or body

New Definitions







- Pseudonymous data
- Encrypted data
- Profiling
- Personal Data Breach
- Genetic Data
- Biometric Data
- Data Concerning Health
- Main Establishment
- Representative
- Enterprise
- Group of Undertakings
- Binding Corporate Rules
- Child

Principles & Processing Conditions

- The Principles now include specific reference to:
 - Being transparent
 - Limiting personal data to the minimum necessary
 - The responsibility and liability of the data controller
- Processing conditions
 - Legitimate Interests condition is narrowed
 - **Legitimate interests cannot be relied upon for secondary purposes**
 - There are specific conditions to be met if relying on consent
 - Explicit
 - Burden of proof on the Data Controller
 - **Cannot be used if there is a significant imbalance between the individual and data controller** Purpose limited
 - The exemptions to the prohibition on processing special categories of personal data now include
 - The establishment, exercise or defence of legal claims
 - Specific provisions relating to **administrative sanctions, judgments, criminal convictions or related security measures**

Information Policies

New symbols to be used at the point of collection

	No personal data are collected beyond the minimum necessary for each specific purpose of the processing	
	No personal data are retained beyond the minimum necessary for each specific purpose of the processing	
	No personal data are processed for purposes other than the purposes for which they were collected	
	No personal data are disseminated to commercial third parties	
	No personal data are sold or rented out	
	No personal data are retained in unencrypted form	

COMPLIANCE WITH ROWS 1-3 IS REQUIRED BY EU LAW

Information to the Individual

- To be provided after the information policy has been provided:
 - Detail the contract terms and legitimate interests if applicable
 - Retention period
 - Right to lodge a complaint and the contact details of the supervisory authority
 - Recipients
 - Intended transfers
 - Profiling
 - Logic
 - Public authority disclosures

Individuals' Rights

- Right of Access
 - One month 40 calendar days
 - Free of charge
 - Where possible, provide via remote access to a secure system
 - Electronic requests
- Right to be Forgotten erasure
 - Not an absolute right
- Data Portability
 - Structured and commonly used format
- Profiling
 - Restrictions
- Rights to object
 - Must be told clearly

Data Controller/Processor Obligations

- Data Protection by Design
- Risk Analysis
- Joint Controllers/Processors
 - Specific recognition
- Specific security obligations
 - (a) the ability to ensure that the integrity of the personal data is validated;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
 - (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;
 - (d) in the case of sensitive personal data processing ...additional security measures to ensure situational awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data;
 - (e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.

Data Controller/Processor Obligations continued

- Personal Data Security Breach Notification
 - Without undue delay **and where feasible, not later than 24 hours, notify the Data Protection Authority**
 - A data processor must inform the data controller **immediately without undue delay** a personal data security breach is discovered
 - Document
 - Where the breach is likely to adversely affect an individual the individual must be notified without undue delay.
- **Impact Assessment Lifecycle Data Protection Management**
 - If there is a specific risk, conduct a data protection impact assessment
 - **Examples of areas of risk are detailed in the GDPR**
- Prior **Authorisation and Consultation**
 - Needed in limited circumstances

Data Protection Officer

- A Data Protection Officer (DPO) must be appointed (Data Controller or Processor)
 - By a public authority or body
 - **By an enterprise employing 250 or more** processing personal data on 5000 or more individuals
 - Where core activities require regular and systematic monitoring of individuals.
 - **Core activities relate to processing sensitive personal data, location data or data on employees in large scale filing systems**
- The DPO must be appointed on the basis of professional qualities and expert knowledge of data protection law and practices and ability
- There must be no conflict of interest in the DPOs duties
- The DPO may be an external appointment
- The appointment must be for a minimum of **two (external appointment) or four (employee)** years

- The DPO can only be dismissed if he/she no longer fulfills the conditions required for performance of duties
- The name of the DPO must be provided to the DPA and the public
- Individuals have the right to contact the DPO
- The DPO must have independence and be supported through the provision of staff, premises, equipment, etc., **and to maintain his or her professional knowledge.**
- **The DPO shall report to a designated executive management member.**
- Advisory and compliance monitoring role.

Certification

Certification

- “European Data Protection Seal”
- Voluntary, affordable, harmonised
- Third parties may be accredited to do the assessment

Personal Data Transfers to Third Countries

- Personal data transfers to third countries or international organisations are allowed:
 - Where there has been an adequacy decision for the country/territory, processing sector or international organisation
 - Where appropriate safeguards are in place:
 - Binding Corporate Rules (can now include external subcontractors)
 - EU Commission approved clauses (i.e. model clauses)
 - Standard DPA approved clauses in accordance with the consistency mechanism
 - Bespoke clauses authorised by a DPA (prior to processing)
- Derogations now include:
 - Legitimate interests of controller or processor as long as the transfers are not frequent or massive, and appropriate safeguards are in place
- Transfers or disclosures not authorised by Union law
 - Third country judgments/decisions not recognised

Sanctions

Administrative sanctions:

- Three levels of fine
 - Up to 250,000 EUR or, if an enterprise, up to 0.5% of the annual worldwide turnover
 - For not properly responding to individuals requests
 - For charging a fee for a subject access request
 - Up to 500,000 EUR or, if an enterprise, up to 1% of the annual worldwide turnover
 - For not providing the requisite information to individuals
 - For not complying with the rights of individuals
 - Up to 1,000,000 EUR or, if an enterprise, up to 2% of the annual worldwide turnover.
 - For processing without legal basis
 - For not adopting internal policies or implementing appropriate measures for demonstrating compliance
 - For not appointing a DPO
 - For not notifying a personal data breach

(Please note the examples given are not exhaustive.)

Sanctions

Sanctions:

- a) A warning in writing in cases of first and non-intentional non-compliance;
- b) Regular periodic data protection audits
- c) A fine up to 100,000,000 EUR or up to 5% of the annual worldwide turnover, whichever is greater.

Contact Details

Melanie Shillito

Director

Promontory Financial Group (UK) Limited

2nd Floor

30 Old Broad Street

London EC2N 1HT

Direct: 020 7997 3411

Mobile: 07841 873282

mshillito@promontory.com

