General Data Protection Regulation

Information session for public sector

Timelines

- Political agreement reached in mid-December
- Text currently being prepared in all languages, and streamlined
- Formal adoption expected in late April or early May
- Will apply from April/May 2018
- Will apply to both public and private sectors
- Regulation with direct effect but which allows for national laws ("hybrid" instrument) which should take effect at the same time

Justifications for data protection reform at EU level

- The Lisbon Treaty introduced a new legal basis for higher data protection standards in the EU (Article 16). The right to data protection is also included in the Charter of Fundamental Rights (Article 8)

- The data protection standards set out in the 1995 Data Protection Directive – on which current data protection law is based – need to be updated to take account of technological advances (Internet; social networking; Big Data) and new business models (cloud computing), i.e. the digital economy

- Rapidly developing case law of Court of Justice on data protection

- Need for more consistent application of data protection law in single digital market points towards a Regulation to replace the 1995 Directive

Exclusions from scope of Regulation

- This Regulation does not apply to the processing of personal data:
  - (a) in the course of an activity which falls outside the scope of Union law ("activities concerning national security")(Recital 14)
  - by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union ("common foreign and security policy")
  - by a natural person in the course of a purely personal or household activity
  - by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; this area is covered by the new Directive

Digital economy: Innovation, growth and jobs – v – human rights

- Technological advances and innovative business models in the digital economy present opportunities for innovation, job creation and economic growth both in Member States and across the Union

- Data protection is about the rights and freedoms of individuals: their rights to control the uses to which their personal data are put and their freedom not to be subjected to unnecessary monitoring or observation

- Data protection rights and safeguards must keep pace with the emerging technologies and new business models; otherwise there will be insufficient consumer trust and confidence in the digital economy to ensure that its jobs and growth potential is fully realised

Impact for business

- Data Protection Regulation will replace 1995 Directive and displace Data Protection Acts 1988 and 2003
- Benefits arising from more harmonised application of data protection law in EU digital market (500 million consumers)
- Benefits arising from more streamlined and less burdensome procedures
- Potential benefits arising from 'one-stop-shop' (OSS) for companies with establishments in more than one Member State, or providing services across the EU from a single establishment
  - Based on 'main' establishment and 'lead' DPA
  - Does not apply to public sector
- Risk of excessive referral of cases to European Data Protection Board arising from the OSS mechanism, resulting in costs and delays; imposition of Board decisions on DPAs

Benefits for individuals

- Stronger obligation on controller to provide information in a transparent and speedy manner, without charge
- Strengthened data subject rights

  - to obtain details about the processing of their personal data, whether received directly from them or from another source

  - to obtain copies of personal data undergoing processing

  - to rectification of incorrect or incomplete data

  - to erasure ("right to be forgotten")

  - to restriction of processing

  - to data portability (new)

  - to object to processing

  - limitation on automated decision making, including profiling

  - to notification of serious data breaches which may involve high risk for their rights and freedoms

Part 1 – What's new in the Regulation?

- More emphasis on transparency
  - Personal data must be processed lawfully, fairly and in a transparent manner: Article 5.1(a)
  - Provide information "in an intelligible and accessible form, using clear and plain language": Article 12

- More emphasis on accountability
  - The controller shall be responsible for and be able to demonstrate compliance with the Regulation: Article 5.2

- More emphasis on security
  - Personal data must be processed in a way that ensures appropriate security of the personal data: Article 5
  - Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk: Article 30

‘Risk-based’ approach to controller obligations (Articles 22 and 30)

- The controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is in compliance with the Regulation, taking into account:
  - the nature, scope, context and purposes of the processing, and
  - the risks of varying likelihood and severity for the rights and freedoms of individuals

Mitigation of risk

- Data protection impact assessments (Article 33)
- Mandatory prior consultation of DPA in cases of identified risks and intended legislation (Article 34)
- Designation of data protection officer; mandatory for public authorities and bodies (Article 35)
- Codes of conduct (Articles 38 and 38a)
- Certification mechanisms and data protection seals and marks (Articles 39 and 39a)

Mandatory reporting of breaches to DPA

- Mandatory reporting of all personal data breaches to DPA unless a breach is unlikely to result in a risk for rights and freedoms of individuals:
  - without undue delay and, where feasible, not later than 72 hours after becoming aware of it
  - report must identify the likely consequences of the breach and the measures taken, or to be taken, to mitigate possible adverse effects for individuals
  - facts surrounding the breach, its effects and remedial action taken must be documented to verify compliance
  - DPA may require notification of all data subjects where a breach is likely to result in high risk for their rights and freedoms

Right to compensation and liability

- A person who has suffered material or non-material damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller for the damage suffered
- Any controller involved in the processing shall be liable for the damage caused by the processing which is not in compliance with the Regulation. A processor shall be liable for damage only where it has not complied with obligations of the Regulation specifically directed to processors or acted outside or contrary to lawful instructions of the controller
- A controller shall be exempted from liability if it proves that it is not in any way responsible for the event giving rise to the damage
- Where more than one controller or processor or a controller and a processor are involved in the same processing and, where they are responsible for any damage caused by the processing, each controller or processor shall be held liable for the entire damage, in order to ensure effective compensation of the data subject
- Where a controller has paid full compensation for the damage suffered, that controller shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage

Need for contract between controller and processor (Article 26)

- Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject

- The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes

- Applies in simple cases (Department's contract with shredding company) and complex cases (Public authority contract with provider of cloud services)

Administrative fines

- Each DPA shall ensure that the imposition of administrative fines in respect of infringements of this Regulation shall in each individual case be effective, proportionate and dissuasive
- Infringements shall be subject to administrative fines up to €10,000,000 or €20,000,000 (or, in case of an undertaking, up to 2% or 4% of the total worldwide annual turnover of the preceding financial year)
- Member States may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies (consultation will be held on this in due course)
- The exercise by DPAs of the power to impose fines shall be subject to appropriate procedural safeguards in conformity with Union and national law, including effective judicial remedy and due process

Designation of data protection officer

- The controller must designate a data protection officer in any case where
  - the processing is carried out by a public authority or body; or
  - the core activities of the controller or processor consist of processing operations which because of their nature, scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
  - the core activities of the controller or the processor consist of processing on a large scale of sensitive personal data.
- A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment
- Where the controller or processor is a public authority or body, a single data protection officer may be designated for several of them, taking account of their organisational structure and size

Data protection officer requirements

- The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and his or her ability to fulfil the tasks
- The data protection officer shall report directly to the highest management level of the controller
- The controller shall ensure that the data protection officer does not receive any instructions regarding the exercise of his or her tasks
- The data protection officer may be a staff member or fulfil the tasks on the basis of a service contract
- The data protection officer may fulfil other tasks and duties as long as such tasks and duties do not result in a conflict of interests

Tasks of data protection officer

- The controller must ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data

- The data protection officer shall have at least the following tasks:
  - to inform and advise the controller and the employees who are processing personal data of their obligations under the Regulation and any other data protection provisions;
  - to monitor compliance with the Regulation, any other data protection provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations;
  - to provide advice as regards the data protection impact assessment and monitor them;
  - to cooperate with the DPA and act as the contact point on issues related to the processing of personal data, including prior consultation

- Data subjects may contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights

Part 2 – Further specific provisions in relation to public sector

- Limitations on lawfulness grounds
- Legal basis may contain more specific provisions
- Objectives of general public interest where restrictions on exercise of data subject rights permitted
- Conditions applicable to restrictions
- Provisions applicable to specific situations:
  - Freedom of expression and information; access to official documents
  - Archiving purposes; statistical purposes; scientific and historical research purposes

Lawfulness of personal data processing

- Article 6.1 outlines the six grounds which render the processing of personal data lawful; these are the grounds which already apply under the 1995 Data Protection Directive and the Data Protection Acts 1988 and 2003:

(a) Consent (unambiguous or explicit depending on whether the data are sensitive)

(b) Necessary for contractual reasons

(c) Necessary for compliance with a legal obligation to which a data controller is subject

(d) Necessary to protect vital interests of an individual

(e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

(f) Necessary for the purposes of the 'legitimate interests' pursued by the controller or a third party (provided such interests are not overridden by the rights and freedoms of individuals)

Restrictions applicable to the public sector

- The public sector will no longer be able to rely on grounds (a) and (f), i.e. the consent and legitimate interests grounds

- Recital 34 states that consent should not provide a valid legal ground for the processing of personal data “where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and this makes it unlikely that consent was freely given in all the circumstances of that specific situation”

- On ‘legitimate interests’ ground, Article 6.1(f) states “This shall not apply to processing carried out by public authorities in the performance of their tasks”

Data processing by public sector

- Processing referred to in (c) and (e) must be laid down in Union or national law; it must meet an objective of public interest and be proportionate to the legitimate aim pursued

- This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia, the general conditions governing the lawfulness of data processing by the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing

- Recital 36: “This Regulation does not require that a specific law is necessary for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient”

Permitted restrictions on exercise of data subject rights

- Article 21 of the Regulation permits limited restrictions on the exercise of data subject rights in order to safeguard important objectives of general public interest:

  (a) national security, defence, public security

  (b) prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (i.e. scope of Data Protection Directive)

  (c) other important objectives of general public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security

  (ca) the protection of judicial independence and judicial proceedings

  (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions

  (e) a monitoring, inspection or regulatory function connected to the exercise of official authority

  (f) the protection of the data subject or the rights and freedoms of others

  (g) the enforcement of civil law claims

Conditions applicable to restrictions

- Article 21.1 - The scope of these permitted restrictions is narrowly drawn:
  - They must be in the form of a legislative measure;
  - respect the essence of fundamental rights and freedoms; and
  - constitute a necessary and proportionate measure in a democratic society

- Article 51.1 of the Charter

  "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others"

Court of Justice of European Union case law

- Schecke (2010) C-92/09 and C-93/09 (Publication of names of CAP beneficiaries and amounts received)
  - EU rules annulled because of inadequate balance between need for transparency and individuals' data protection rights; lack of proportionality

- Digital Rights Ireland (2014) C-293/12 and C-594/12 (Retention of data by telecom providers)
  - Data Retention Directive annulled because of lack of proportionality between retention of traffic and location data and individuals' rights to privacy and data protection; the interference with these rights was not sufficiently circumscribed to ensure that it was limited to what was strictly necessary

- Schrems (2015) C- 362/14 (transfers of personal data to US companies)
  - 'Safe Harbour' Adequacy Decision declared invalid; protection of fundamental rights at EU level "requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary" (paragraph 92)

- Irish courts bound by Court of Justice case law, or may opt to refer questions to the Court

Content of legislative measures

- Legislative measures must “contain specific provisions at least, where relevant, as to:

  (a) the purposes of the processing or categories of processing,

  (b) the categories of personal data,

  (c) the scope of the restrictions introduced,

  (d) the safeguards to prevent abuse or unlawful access or transfer;

  (e) the specification of the controller or categories of controllers,

  (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

  (g) the risks for the rights and freedoms of data subjects; and

  (h) the right of data subjects to be informed about the restriction, unless this may be prejudicial to the purpose of the restriction”

Freedom of expression

- ***Processing of personal data and freedom of expression and information***

  Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression (Article 80)

- ... In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly (Recital 121)

Freedom of information

- ***Processing of personal data and public access to official documents***

  Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union law or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation (Article 80a)

- This Regulation allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Regulation. Public access to official documents may be considered as a public interest (recital 121a)

Archiving; statistical purposes; historical and scientific research purposes

- Article 5(b) permits further processing of personal data originally collected for a specified purpose for the above purposes in breach of the “purpose limitation” principle; in like manner, paragraph (e) permits storage for longer periods than justified in relation to the original purpose in breach of the “storage limitation” period. In both cases, the further processing is expressed to be subject to Article 83

- Article 83 permits further processing for these purposes subject to appropriate safeguards for the rights and freedoms of individuals. These safeguards require that technical and organisational measures be put in place in order to ensure respect for the “data minimisation” principle. These measures may include “pseudonymisation” of the data provided that this does not defeat the purpose of the further processing

- Article 83 also permits the imposition of restrictions, subject to the safeguards referred to above, on the exercise of certain data protection rights of individuals in so far as such rights are likely to render impossible or seriously impair the achievement of the purpose of the further processing

Health research and scientific research

- By coupling information from registries, researchers can obtain new knowledge of great value when it comes to e.g. widespread diseases such as cardiovascular disease, cancer, depression etc. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about long-term impact of a number of social conditions e.g. unemployment, education, and the coupling of this information to other life conditions. Research results obtained on the basis of registries provide solid, high quality knowledge, which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people, and improve the efficiency of social services etc. In order to facilitate scientific research, personal data can be processed for scientific research purposes subject to appropriate conditions and safeguards set out in Union or national law (Recital 125a)

- For the purposes of this Regulation, processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research, privately funded research and in addition should take into account the Union's objective under Article 179(1) of the TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes (Recital 126)

Next steps

- Departments and Offices will need to examine legislation (statutes and statutory instruments), including legislation establishing subsidiary bodies and their activities, and amend where necessary in order to ensure compliance with the Regulation's obligations and data protection safeguards

- New legislation may be required to fill gaps where no statutory provisions currently exist (e.g. in relation to any activity based on profiling, or scientific research activities)

- Any new legislation will need to be in place by April or May 2018 in order to withstand legal challenges grounded on non-compliance with EU data protection law

- Put compliance with Regulation into strategic plans and risk registers