THE GENERAL DATA PROTECTION REGULATION: A BRIEF OVERVIEW (*)

The first IBM Personal Computer was introduced just over 35 years ago, on August 12, 1981. The first-generation iPhone was introduced in the United States on June 29, 2007. In the intervening decade the humble 'cell-phone' has become a multi-media device for surfing the web, checking email, taking and sharing photographs. Facebook launched in 2004 and Twitter in 2006. Beginning from the mid-1980s the volume of personal communications via electronic means has increased exponentially.

Online platforms and internet browsers are 'free' to use. But users are requested to give their personal data in exchange. There is an apparent tension between individuals' right-to-respect for their private and family life, home and correspondence and the ambition of companies to reach new customers in more targeted and effective ways.

As the technology has advanced legislation has struggled to keep pace. The Council of Europe Convention for the 'Protection of Individuals with regard to the Automatic Processing of Personal Data' was adopted in Strasbourg on 28 January 1981. A first Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was implemented from October 1998.

Directive 95/46/EC will be repealed and replaced by the General Data Protection Regulation ("**GDPR**") which will apply from 25th May 2018. The ambition of the GDPR is to up-date the EU's data protection law and make it relevant to the twenty-first century. It is a piece of complex legislation. The preamble to the GDPR has one hundred and seventy-three recitals. There are ninety-nine articles split between ten chapters. A brief overview of the new legislation is set out below. (References are to the articles of the Regulation unless otherwise stated).

Definitions A. 4

- **Personal data** is defined in A. 4.1, it means any information relating to an identified or identifiable natural person ('data subject') and includes references to an identifier such as a name, an identification number, location data or an online identifier of that person.
- **Data Controller** means the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data, A. 4.7.
- **Data Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller, A. 4.8.

Scope AA. 2 & 3

- **Material scope**: The GDPR applies to processing of personal data, whether wholly or partly by automated means and also to manual processing of personal data which form part of a filing system or is intended to form part of a filing system. (Exceptions are found in A. 2.2.)
- **Territorial scope**: The territorial scope of the GDPR is very broad. It applies to all data processing activities of controllers or processors established within the EU processing, regardless of whether the processing takes place in the EU or not. It also applies to all companies worldwide that process personal data of EU citizens to offer them goods or services or monitor their behaviour within the EU.

Data processing principles

- **Article 5** stipulates familiar principles relating to processing of personal data. Including principles of Lawfulness, Fairness and Transparency and that data shall be collected for a specified purpose, shall be proportionate to that purpose and accurate ('purpose limitation', 'data minimisation' and 'accuracy').
- **The important new principle of 'accountability'** is introduced in A. 5.2. The requirement is that the data controller shall be responsible for, and be able to demonstrate, compliance with the processing principles.

Lawfulness of processing

- **Lawfulness of processing**: A.6 sets out six grounds that may underpin lawful processing in any particular case. These include where processing is necessary for the performance of a contract, processing necessary for compliance with the legal obligation to which the controller is subject and processing necessary for purposes of legitimate interests pursued by the controller.
- **Consent**: is one of the six grounds for lawful processing. Any such consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her, A.7. It shall be as easy to withdraw as to give consent.

Rights of the data subject AA. 12-23

- As noted above, transparency is a key data processing principle.
- Data subjects can expect to receive transparent information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language. (AA. 12,13 and 14)
- The requirement for transparency is under-pinned by a number of specific rights by which the data subject can ensure fair processing of their personal data. A.15 Right of access to personal data by data subject (article 15). A.16. Right of rectification, A Right to erasure ('*right to be forgotten*'): Organizations have to ensure they have the processes and technologies in place to delete data in response to requests from data subjects, A.17. Right to restriction of processing & Right to data portability AA. 18 & 20.
- There is a clear limitation on profiling in A22. The data subject has the right not to be subject to a decision that produces legal effects concerning him or her based solely on automated processing, including profiling.

The controller and processor AA. 24-32

- **Responsibility of the controller A.24.** The controller shall take appropriate technical and organizational measures to ensure and to be able to demonstrate that processing of personal data is carried out in accordance with the GDPR.
- **N.B.** *Under A. 30 each controller shall maintain a record of processing activities carried out under its responsibility*. This requirement may (subject to conditions) be to disapplied in the case of small or medium-sized companies, employing fewer than 250 people; the Belgian data protection supervisory authority has said it regards it as good practice for all companies to maintain such a register.
- **Responsibility of the processor**: the GDPR extends liability to processors who do not comply with the requirements of the Regulation. **Ensuring security of processing** through technological and organizational means, including, as appropriate, by pseudonymisation and encryption of personal data, is a mandatory compliance requirement for both data controller and processor, within the boundaries of the state-of-the-art, the costs of implementation and the risks the processing poses for data subjects.

Compliance tools

- The GDPR includes certain compliance tools. **A. 25 Data protection by design and by default.** Broadly speaking the intention of this provision is that, instead of thinking about data protection issues at the end of designing or implementing new tools or processes, the requirement to respect data protection principles and the requirements of the GDPR must be built in from the conception of such tools or processes.
- **AA.33 & 34 Notification of data breach.** The data breach notification requirements are intended to harmonise practice with in the EU.
- **Data protection impact assessment A.35**. Where a type of processing poses high privacy risks for data subjects (for example when introducing a new technology) organisations will have to conduct a privacy risk assessment and may need to work with the competent regulatory authority to ensure compliance with GDPR.

Data protection officer ('DPO') A. 37

- **Designation of a DPO** is mandatory in certain cases, in particular where processing is carried out by a public authority or body, except for courts acting in their judicial capacity. It is possible for a group of undertakings to appoint a single data protection officer provided that this DPO is easy accessible from each establishment.
- According to a study by the international association of privacy professionals, this requirement will mean that 28 000 DPOs will have to be appointed in Europe.
- The DPO can be natural person or a legal person. If a legal person it is essential that every member of that organization who functions as a DPO does so in accordance with the rules of AA. 37-39.

Codes of conduct and certification AA. 40-43

- Instruments to demonstrate compliance.
- Codes of conduct AA. 40-41 and Certificates AA. 42-43) are expressly recognized by the Regulation as being acceptable mechanisms adherence to which will be a means of demonstrating GDPR compliance. At the time of writing these are still in a development stage.

Transfers of personal data to third countries or international organizations AA. 44-50

- A.44 sets out the general principle that transfers outside the EU shall only take place if the requirements of these provisions are met.
- A. 45.3 stipulates that the EU Commission may decide that a third country provides an adequate level of personal data protection so that transfers to that country may take place without further authorization.
- In the absence of an adequacy decision as mentioned above, a controller or processor may only transfer personal data to a third country if they provide appropriate safeguards. These can be provided by a number of mechanisms including binding corporate rules (A. 47) or by the use of, by standard contractual clauses.

Supervisory authorities AA. 51-59

- Each state shall have one or more independent public authorities, who will be responsible for monitoring compliance with the GDPR. Their competence tasks and powers are set out in AA. 55-58
- **One stop shop principle**: For cross border data transfers within the EU there will be one lead data protection supervisory authority ('DPSA'). The presence of the main establishment (meaning the place of central administration) of an entity will, in principle, indicate where the lead supervisory authority is located. But this is subject exceptions and any DPSA shall be competent to handle a complaint whose subject matter only concerns the member state for which it has responsibility.

Cooperation and consistency AA. 60-67 and the European Data Protection Board AA. 68-76

- To ensure a consistent level of application of the GDPR the DPSAs will be required to cooperate with each other and with the EU Commission through a consistency mechanism.
- The European Data Protection Board; it is an independent body with legal personality. It's composed of representatives of the DPSA's from each Member State and of the European Data Protection Supervisor. The Board has the task of dispute solving and shall adopt binding decision in certain cases.

Remedies, liability and penalties AA. 77-84

- **The ex-post risks of non-compliance with the GDPR are significant**. Certain breaches of the GPDR can be the subject of administrative fines of up to 4% 20 million Euros or 4% of the annual global turnover of the entity concerned, whichever is higher, A. 83.6. This is the maximum fine, which will be imposed for the most serious infringements (for example of data subjects' rights). The maximum fine for (procedural) infringements, considered to be less serious, is limited to 2% of annual worldwide turnover or 10 million Euros.
- **Remedies available to data subjects include**: the right to lodge a complaint with a DPSA, the right to an effective judicial remedy against a DPSA and the right to an effective judicial remedy against a controller of processor.
- **Right to compensation**. Every person who has suffered material (financial) or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or the processor for the damage suffered.

AA. 85-91 set out provisions relating to specific processing situations

- **A.88 concerns processing of employee data**. It allows room for the member states to provide more specific employment rules by law or by collective agreements.

AA. 92-99 concern implementation of the GDPR

A. 99 2. Provides that the GDPR shall apply from 25 May 2018.