

Data Protection: The proposed Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Introduction

This article deals with the proposed new legal framework for the protection of personal data in the European Union ('EU'). The European Commission ('Commission') carried out extensive consultations with all major stakeholders on a review of the current legal framework for the protection of personal data. The scale and ways in which personal data are collected, accessed, used, shared and transferred have undoubtedly been transformed by the rapid pace of **changes in technology** and the **effect of globalisation**. As a result of the consultation, the Commission had to take steps to bring the data protection laws up-to-date to meet the challenges of these technological changes. Personal data are collected, transferred and exchanged in large volumes across the world and there has to be safeguards in place to protect such data. For instance, new challenges are posed by the advent of cloud computing (where individuals access computer data remotely) for the current data protection laws, as data are transferred across the globe. The laws on data protection have to be brought in line with technological developments. The Regulation goes a long way in clarifying the law and is a good piece of legislation.

The aim of the Regulation is:

- To encourage consumers to purchase **online in full confidence that their data will be protected**. It is envisaged that the lack of trust makes consumers hesitant to buy online and adopt new services.
- **To encourage consumers** to embrace new technologies.
- To provide a **greater choice of goods at lower prices** for consumers.
- **To increase online activity** to aid businesses, especially small and medium-sized businesses (SMEs), to **grow to their full potential** within the EU.
- To create **certainty** about data protection issues online for individuals and businesses.
- To **build trust in the online environment**.
- To create **consistency** of data protection enforcement in the EU.
- To improve the **efficiency of data protection supervision and enforcement** across the EU.

What is the proposal?

The proposal is for a single Regulation across the EU to safeguard the security of individual's personal data and to have the fundamental rights of individuals to data protection respected. It proposes new rights, for example:

- The **'right to be forgotten'** - meaning that if an individual no longer wishes for his/her personal data to be processed, and there is no legitimate reason for such data to be retained by a data controller, the data **must** be deleted from the organisation's system;
- The **right to data portability** - meaning the individual's right to obtain a copy of his/her data from an Internet company and to be able to forward it to another online company without any restrictions.
 - ❏ For example, where an individual has stored photographs, personal messages and personal contacts on a social networking site (photo-sharing site), if the individual decides to move to a new site, the individual would have the right to transfer all such photographs and data (where technically possible), without any restrictions or loss of data.
- Ensuring **easy access to one's own data**.
- Ensuring that **consent** of the individual whenever is required for the processing of personal data **is given explicitly**.
- Ensuring a **single set of rules** applicable throughout the EU.
- **Clear rules** on **when EU law would apply to data controllers outside the EU**.

The EU has proposed two new legal framework:

- A proposal for a Directive with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and
- A proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

New Elements of the Data Protection Principles

The Regulation will introduce the following new elements:

- The **transparency** principle.
- The **data minimisation** principle.
- The establishment of a comprehensive **responsibility and liability of the controller**.
- The criteria for **lawful processing**.
- The conditions for **consent** to be valid as a legal ground for lawful processing.
- The conditions for the **lawfulness of the processing** of personal data of children in relation to information society services offered

directly to them.

- **Prohibition for processing** special categories of personal data and the exceptions from this general rule.
- Data controller not obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of the Regulation.
- Data controllers to provide **transparent and easily accessible and understandable. Information.**
- Data controller to provide **procedures and mechanism** for exercising the data subject's rights, including means for electronic requests, requiring response to the data subject's request within a defined deadline, and the motivation of refusals.
- Obligation on data controllers to data subjects to **provide additional information** on:-
 - ❏ storage periods.
 - ❏ the right to lodge a complaint.
 - ❏ the right to access to personal data.
 - ❏ the right to rectification.
 - ❏ the right to erasure.
 - ❏ the right to be forgotten.
 - ❏ the right to have the processing restricted in certain cases.
 - ❏ the right to data portability - the right to obtain such data in a structured and commonly used electronic format.
 - ❏ the right to object to direct marketing.
 - ❏ the right not to be subject to a measure based on profiling.
 - ❏ the right of any data subject to lodge a complaint with a supervisory authority.
 - ❏ the right of judicial remedy against a supervisory authority.
- The obligation on a data controller who has made personal data public to inform third parties (on the data subject's request) to erase any links to, or copy or replicate that personal data.
- A data processor that processes data beyond the data controller's instructions is to be considered as a joint controller.
 - ❏ the obligation on the data controller and processor to maintain documentation of the processing operations under their responsibility.

- The obligation on [data controller and the processor](#):
 - ✚ to implement appropriate measures for the security of processing (obligation is now extended to a data processor, irrespective of the contract with the controller).
 - ✚ to carry out a data protection impact assessment prior to risky processing operations.
- An obligation on data controller to notify personal data breaches.
- An obligation to appoint a mandatory data protection officer for the public sector, and, in the private sector, for large enterprises or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring.
- Introduces the possibility of establishing certification mechanisms and data protection seals and marks.
- For transfer of personal data to third countries, where no adequacy decision has been adopted by the Commission, to adduce appropriate safeguards, in particular, standard data protection clauses, binding corporate rules and contractual clauses.
- Conditions for processing personal data for historical, statistical and scientific research purposes.
- The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, would not fall within the scope of this Regulation.
- The principle of public access to official documents is allowed.
- A data controller not established in the EU should be subject to the provisions of the Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.
- In order to determine whether a processing activity can be considered to '[monitor the behaviour](#)' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing devices which consist of applying a 'profile' to an individual, specifically, to take decisions concerning the individual or for analysing or predicting the individual's personal preferences, behaviours and attitudes.
- The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account would be taken of all means the data controller is likely to reasonably use either by the data controller or by any other person to identify the individual.

- The principles of data protection would not apply to 'anonymized' data so that the data subject is no longer identifiable.
- When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.
- Consent should be given explicitly *'...by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided...'*
- Personal data relating to health should include in particular
 - ✚ all data pertaining to the health status of a data subject
 - ✚ information about the registration of the individual for the provision of health services
 - ✚ information about payments or eligibility for healthcare with respect to the individual
 - ✚ a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes
 - ✚ any information about the individual collected in the course of the provision of health services to the individual
 - ✚ information derived from the testing or examination of a body part or bodily substance, including biological samples
 - ✚ identification of a person as provider of healthcare to the individual
 - ✚ or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.
- Children deserve specific protection of their personal data, as they

may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data.

© RT COOPERS, 2013. This Briefing Note does not provide a comprehensive or complete statement of the law relating to the issues discussed nor does it constitute legal advice. It is intended only to highlight general issues. Specialist legal advice should always be sought in relation to particular circumstances.

Author: Rosanna Cooper. Contact enquiries@rtcooperssolicitors.com or 0207 488 9947