General Data Protection Regulation

The protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data

Part 1 of an Article By Dr Rosanna Cooper and Ebby John

Introduction

This article deals with the provisions of **Regulation (EU) 2016/679 referred to as the** General Data Protection Regulation ("GDPR") in connection with the protection of **personal data** in the European Union ('EU'). The GDPR will come into force on 25 May 2018 and will repeal Directive 95/46/EC with effect from 25 May 2018. The GDPR does not apply to the personal data of deceased persons. The highlighted areas are extracts from the GDPR:

> The protection afforded by this Regulation should **apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data**. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

The changes brought about by globalisation and the rapid paces of changes in technology have impacted on how personal data are **collected, accessed, used, shared and transferred**. The GDPR is intended to meet the challenges of these technological developments and global changes.

> The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

Personal data are collected, transferred and exchanged in large volumes across the world and the GDPR ensures that there are safeguards to protect such data, for instance, to address the challenges posed by the advent of

cloud computing (where individuals access computer data remotely), as data are transferred across the globe.

> **Rapid technological developments and globalisation have brought new challenges for the protection of personal data**. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

The processing activities are related offering goods or services to data subjects irrespective of whether connected to a payment:

> In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to **offering goods or services to such data subjects irrespective of whether connected to a payment**. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Unio

Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. **Processing must be Lawful and Fair**

Definitions

Some key definitions under Article 4 of the GDPR are:

'**personal data**' is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'**processing**' is defined any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

'**consent**' of the data subject means any 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.

'**personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Processing

Article 2 (1) of the GDPR, applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

The GDPR does not apply in the following circumstances (Article 2(2)):

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;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the 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.

The territorial scope of the GDPR under Article 3 (1), states that the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU is **regardless of whether the processing takes place in the Union or not**.

According to Article 3 (2), the GDPR applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- The monitoring of their behaviour as far as their behaviour takes place within the Union.
- This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

In order for processing to be lawful, personal data should be **processed** on the basis of the **consent** of the data subject concerned. Where **processing** is based on the **data subject's consent**, the **controller** should be able to **demonstrate that the data subject has given consent to the processing operation**. In particular, in the context of a written declaration on another matter, safeguards should ensure that the **data subject is aware of the fact that and the extent to which consent is given**.

Sensitive Data

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation.

Research

Data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Data Protection Principles

The Principles relating to processing of personal data (Article 5) are as follows:

1. Personal data shall be:

(a) **processed lawfully, fairly and in a transparent manner in relation to the data subject** ('lawfulness, fairness and transparency');

(b) **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed** ('data minimisation');

(d) **accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay** ('accuracy');

(e) **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed**; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures** ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Part 2 to follow:

DR Rosanna Cooper is a specialist in data protection and now the GDPR. Ebby John acts as a consultant to RT Coopers and is a GD{R specialist.