

DATA PROTECTION: THE EU REFORM PROPOSALS

Timothy Pitt-Payne QC

INTRODUCTION

1. The Commission's reform proposals are set out in detail at:

http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

They were announced on 25th January 2012. The proposals consisted of two main elements: a draft Regulation, dealing generally with data protection (the General Data Protection Regulation); and a draft Directive relating to the processing of personal data within the criminal justice system.

2. This paper focuses on the proposed General Data Protection Regulation (and in particular its first four chapters), explaining the background and context of the proposals, and some of their main implications for individuals, and for organisations in the private and public sector that handle personal data. The draft Regulation, with an accompanying explanatory memorandum ("the Memorandum"), is at:

http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf

3. The proposals are the outcome of over two years' work at EU level, and it is likely to be at least a further two years before they come into effect. The UK's Ministry of Justice has issued a call for evidence (ending on 6th March 2012) seeking views about the likely impact of the proposals, and in particular their economic implications. For anyone wishing to influence the final form of the legislation, this is a crucial opportunity.
4. As is well known, the main element of the EU's current data protection regime is a 1995 Directive (95/46/EC), given effect in the UK by the Data Protection Act 1998. The Directive referred to two objectives: the protection of the right to privacy, recognised under article 8 of the Convention (see recital 10); and the removal of barriers to the cross-border flow of personal information, resulting from different standards of legal protection within the EU (see recital 8). Under the Commission's proposals, the Directive would be repealed, and the new Regulation would replace it.

CONTEXT FOR THE PROPOSALS

5. The last 20 years have seen fundamental changes in our relationship with information. The internet is now at the heart of business, political and social life. Email is ubiquitous, at home and in the workplace. Internet access is no longer tied to the home or the office, with the development and widespread adoption of smart phones. Individuals voluntarily share a vast amount of personal information online, particularly via social networking sites. And meanwhile it becomes ever easier to store large volumes of personal information: as HMRC notoriously illustrated in November 2007, by losing 2 CDs containing the child benefit records of 25 million individuals. All of these developments have wide-ranging implications for information privacy. They enable personal information to be stored, used and disseminated at an unprecedented scale and speed.

6. What was the situation in 1995, when the Directive was introduced? By way of illustration:
 - The world wide web was already in existence, but there were only about 20,000 websites (see <http://www.zakon.org/robert/internet/timeline/>).
 - You could not have used Google to browse the nascent web. The company was not incorporated until 1998.
 - You could not have sent an email via a web-based email service: for example, Hotmail only started in 1996, and Yahoo's email service began in 1997. Nor could you have browsed the web using a mobile phone.
 - Social networking sites were well into the future. Facebook, for instance, was not launched until 2004.
 - Amazon sold its first book in July 1995, about 3 months before the Directive was introduced.

7. It is unsurprising, then that the Memorandum introducing the proposed changes refers to the pace of technological change, and to the dramatic increase in the use and dissemination of personal information. The draft Regulation is ostensibly intended to protect individuals against the associated threats to their personal privacy. At the same time, there is clearly an economic objective. According to the Memorandum:

Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services.

LEGAL BASIS AND FORM

8. The legal basis of the proposed Regulation is Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), introduced by the Lisbon Treaty. This reads:

1. *Everyone has the right to the protection of personal data concerning them.*
2. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

9. A key aspect of the proposal is that it involves a Regulation, not a Directive (and will therefore be directly applicable, under Article 288 TFEU). The Memorandum seeks to justify this choice of legal instrument, on the basis of reducing legal fragmentation and an increase in legal certainty. Underlying this there appear to be two concerns: that the 1995 Directive was implemented in different ways by different member states; and that businesses operating across the EU have to deal with different national regulators, which may take a widely different approach. Of course, the danger of a desire for common legal standards is that it may lead to the imposition of a solution that is inflexible and unduly prescriptive.

10. In many respects, the Regulation follows the structure of the existing Directive. For instance, it is intended to protect the data of natural persons, but not legal persons. It does not extend to information about the deceased. The Regulation imposes duties on data controllers in relation to their processing of personal data. These include a set of fundamental principles comparable to those set out in article 6 of the 1995 Directive (and currently reflected in Schedule 1 to the 1998 Act). Data processing is legitimate only if certain criteria are met (compare article 7 of the 1995 Directive, and Schedule 2 to the 1998 Act). Certain special

categories of data are identified (compare article 8 of the 1995 Directive, and the categories of “sensitive personal data” in section 2 of the 1998 Act); and these can only be processed for limited, specified bases. In many respects, then, the fundamental structure of the data protection regime will remain unchanged. For someone familiar with the existing regime, the overall structure will seem familiar: but much of the individual content will be strikingly new. In the remainder of this paper I look at the first four chapters in the draft Regulation, identifying the key changes from the existing regime.

CHAPTER 1 - GENERAL PROVISIONS

11. This chapter roughly corresponds with chapter 1 of the 1995 Directive. It defines the scope of the Regulation, its range of application, and its fundamental concepts.
12. The Regulation 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 do so: Article 2.1. This is identical to the definition in Article 3.1 of the 1995 Directive, and the definition of “filing system” remains unchanged. So on the face of it the application of the Regulation to paper records should not be significantly wider than under the current regime.
13. There are various exclusions set out in Article 2.2, including one (article 2.2(d)) in respect of processing of personal data:

By a natural person without any gainful interest in the course of its own exclusively personal or household activity.

This is very similar to the equivalent exclusion in the existing Directive (at Article 3.2), though the specific reference to the absence of gainful interest is new. The Regulation misses the opportunity to grapple with the notorious decision in *Lindqvist*, which held that the posting on a home-made website of personal data about third parties came within the scope of the EU data protection regime, because the website was universally accessible via the internet. The internet is now full of user-generated content (especially on social networking sites), and for many people this kind of activity is part of their social and personal life: so should it come within the scope of EU data protection law? Clearly, companies operating social networking sites ought to be caught by the new Regulation: but should their individual users also be caught?

14. The territorial scope of the Regulation (article 3) is striking. The Regulation applies, unsurprisingly, to the processing of personal data in the context of the activities of an establishment of a controller or processor in the EU (article 3.1). But it also applies to the processing of personal data of EU residents, by a controller not established in the EU, where the processing activities are related to the offering of goods or services to EU residents, or the monitoring of their behaviour. So if a US based search engine monitors the activities of its EU users, or an Australian social networking site allows EU residents to join, then both will be governed by the Regulation in relation to this part of their activities.

15. Personal data, as before, means any information relating to a data subject (Article 4(2)). A data subject is:

An identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The definition is similar to that in the existing Directive, but the specific references to location data, online identifiers and genetic information are new.

16. Although many of the definitions in Article 4 are similar to those in the existing Directive, there are two important departures. There is a specific definition of “consent” (Article 4(8)):

'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

There is also a definition of “personal data breach” (Article 4(9)), as meaning:

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;

CHAPTER 2 - PRINCIPLES

17. This sets out the fundamental principles with which data controllers must comply. The corresponding aspects of the 1995 Directive are given effect in the 1998 Act by: the Data Protection Principles (Schedule 1); the definition of sensitive personal data (section 2); the conditions for lawful processing of ordinary (Schedule 2) and sensitive (Schedule 3) personal data.
18. Article 5 sets out the following principles:

Personal data must be:

- (a) *processed lawfully, fairly and in a transparent manner in relation to the data subject;*
- (b) *collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;*
- (c) *adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;*
- (d) *accurate and 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;*
- (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 data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;*
- (f) *processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.*

19. Article 6 sets out the general conditions for lawful processing. The main points of difference with the existing regime are in relation to consent, and processing by public authorities.
20. As far as consent is concerned, although the data subject's consent is still a basis for lawful processing, the circumstances in which it can be relied upon are narrowed. First, "consent" is specifically defined in Chapter 1: see above. Secondly, there are a new set of "conditions for consent" (Article 7), as follows:

1. *The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.*
2. *If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.*
3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.*
4. *Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.*

The fourth point, I would suggest, is particularly important in relation to the processing of personal data by an employer.

21. Article 8.1 introduces a further specific limitation in relation to consent provided by a child:

For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

22. As to the position of public authorities, the Regulation retains a condition broadly similar to that set out in Schedule 2, paragraph 6 to the 1995 Act. Article 6(f) provides that processing is lawful if it is necessary:

for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

But it then goes on to provide:

This shall not apply to processing carried out by public authorities in the performance of their tasks.

Public authorities will need to rely on the other conditions specified, including condition (e):

processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

23. The Regulation retains a category of what UK law has termed “sensitive personal data” (see Article 9) - e.g. Health information - and this can only be processed on the specific grounds set out in Article 9. These include individual consent (Article 9(a)), but subject to the limitations already set out in the Regulation as to the scope for relying on consent.
24. It is difficult to see how an employer can rely on consent in relation to the processing of sensitive data about an employee (e.g. Health records), given the Regulation’s approach to consent. There is, however, a specific employment-related condition for the processing of sensitive personal data (Article 9(b)):

processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Member State law providing for adequate safeguards

Another potential basis for the lawful processing of sensitive personal data is in Article 9(e):

the processing relates to personal data which are manifestly made public by the data subject

CHAPTER 3 - RIGHTS OF THE DATA SUBJECT

25. This chapter confers six main rights on data subjects:

- (i) A right to the provision of information at the time of collection.
- (ii) A right of access to information that is being processed.
- (iii) Rights in relation to erasure.
- (iv) A right to data portability.
- (v) Rights to object to processing.
- (vi) Rights in relation to profiling.

26. Article 14 deals with the provision of information to the data subject. It builds on the existing provisions relating to fair processing information, but the information required is more detailed than under the current regime. Where personal data relating to a data subject are collected, the controller must provide the data subject with at least the following information:

- (a) *the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;*
- (b) *the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);*
- (c) *the period for which the personal data will be stored;*
- (d) *the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;*
- (e) *the right to lodge a complaint to the supervisory authority and the contact details of*

the supervisory authority;

(f) the recipients or categories of recipients of the personal data;

(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

27. The right of access for the data subject is addressed at Article 15. The data subject has the right, on request, to obtain: (i) confirmation whether personal data relating to him are being processed; (ii) various specified information in relation to the processing; and (iii) communication of the data undergoing processing. There are supplementary provisions in connection with the exercise of this right (see Article 12). The controller has one month to provide the requested information, though this period may be extended by a further month if several data subjects exercise their rights, and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort by the controller (Article 15.2). If the controller refuses to take action, he must inform the data subject of the reasons for refusal and the possibilities of complaining to the supervisory authority (i.e. in the UK, the ICO) and seeking a judicial remedy (Article 15.3).
28. There is a little relief for the hard-pressed data controller in Article 15.4. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may either charge a fee, or refuse to implement the request: but the controller bears the burden of proving the manifestly excessive character of the request.
29. Chapter 3, section 3, has attracted considerable attention, especially in relation to the so-called “right to be forgotten”. The data subject has the right to rectification of inaccurate data (Article 16). There is also a separate right to require erasure of personal data relating to them and the abstention from further dissemination of the data “especially in relation to personal data which are made available by the data subject while he or she was a child” (see article 17). This right may be exercised where one of the following grounds applies:

- (a) *the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
- (b) *the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;*
- (c) *the data subject objects to the processing of personal data pursuant to Article 19;*
- (d) *the processing of the data does not comply with this Regulation for other reasons.*

30. The data controller must carry out the erasure without delay, except where retention is necessary in five specified circumstances (Article 17.3):

- (a) *for exercising the right of freedom of expression in accordance with Article 80;*
- (b) *for reasons of public interest in the area of public health in accordance with Article 81;*
- (c) *for historical, statistical and scientific research purposes in accordance with Article 83;*
- (d) *for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;*
- (e) *in the cases referred to in paragraph 4.*

31. Article 17.4 sets out four circumstances where the data controller should restrict access to data, rather than erasing them:

- (a) *their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;*
- (b) *the controller no longer needs the personal data for the accomplishment of its task*

but they have to be maintained for purposes of proof;

(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

32. Article 18 confers a right to data portability: this will enable the data subject to obtain his personal data from a data controller, and transfer it into another system. The right applies only where the data are processed in a structured and commonly used format, and where the processing is based on consent or on a contract.

33. Article 19 gives data subjects a right to object to the processing of their personal data, where it is based on Article 6(1)(d), (e) or (f). The objection must be upheld unless the data controller demonstrates compelling legitimate grounds for the processing, which override the interests or fundamental rights or freedoms of the data subject. In relation to direct marketing: (i) the data subject has the right to object free of charge to the processing of their data for such marketing; and (ii) this right must be clearly offered to the data subject in an intelligible manner.

34. Finally, Article 20 confers a right to object to measures based on automated processing.

35. Chapter 3, section 5 sets out circumstances in which member states may restrict the scope of the above rights by way of legislative measure.

CHAPTER 4 - CONTROLLER AND PROCESSOR

36. The draft Regulation continues to use the concepts of “data controller” and “data processor”; and the controller is responsible for adopting measures to secure compliance with the Regulation (article 22.2).

37. The Regulation imposes a number of duties on controllers and processors, with the main ones being as follows.

(1) Article 23: data protection by design and by default. Essentially, compliance with

the Regulation must be built into the data controller's systems from the outset.

- (2) Article 25: data controllers not established in the EU, but who fall within regulation 3(2), must designate a representative in the EU (subject to the exceptions in article 25.2).
- (3) The controller and processor must adopt appropriate security measures (Article 30).
- (4) Data breaches must be notified both to the supervisory authority (article 31) and the data subject (article 32).
- (5) The controller and processor must designate a data protection officer (article 35), in three situations:
 - the processing is carried out by a public authority or body;
 - the processing is carried out by an enterprise employing 250 persons or more;
 - the core activities of the controller or processor consist of processing operations requiring regular and systematic monitoring of data subjects.

Timothy Pitt-Payne QC
February 2012