The European data protection framework for the twenty-first century

Viviane Reding*

Abstract

- This article sets out some of the key elements of the Commission's EU data protection reform proposals and highlights a number of the main changes compared to the current situation.
- The new legislative instruments contain important changes to the current acquis, relating in particular to
  - the new legal basis;
  - the choice of legal instruments, including their scope of application;
  - reinforcing the rights of data subjects;
  - enhancing the responsibility of controllers and processors;
  - facilitating international transfers of personal data;
  - guaranteeing independent enforcement; and
  - ensuring protection of personal data by police and criminal justice authorities.

Introduction

On 25 January 2012 the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules. The reasons behind this important initiative had earlier been set out by the European Commission.[1]

This article sets out some of the key elements of the EU data protection reform package adopted by the Commission and highlights a number of the main changes in comparison to the current situation.

Key elements of the EU data protection reform

Proposals for two legislative instruments form the core of the personal data protection reform package: a Regulation,[2] setting out the general EU framework for data protection; and a Directive[3] for the police and criminal justice sector.[4]

Broadly speaking, the Commission's proposals update and modernize well-known and proven general principles enshrined in the 1995 Data Protection Directive.[5] The proposals are also characterized by a

* Vice-President of the European Commission, EU Commissioner responsible for Justice, Fundamental Rights and Citizenship. The author would like to thank Mr Thomas Zerdick, LL.M. for his contribution to this article.

1 See Viviane Reding, 'The upcoming data protection reform for the European Union' (2011) 1/1 International Data Privacy Law 3; European Commission Communication, 'A comprehensive approach on personal data protection in the European Union' COM (2010) 609 final.

2 'Proposal for a Regulation of the European Parliament and of the Council 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)' COM (2012) 11 final ('the Regulation').

3 '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' COM (2012) 10 final ('the Directive').

4 The Commission's package includes the following other documents: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions 'Safeguarding Privacy in a Connected World—A European Data Protection Framework for the 21st Century' COM (2012) 09 final; Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (including annex), COM (2012) 12 final; Impact assessment (including annexes) accompanying the proposed Regulation and the proposed Directive, SEC (2012) 72 final; Executive summary of the impact assessment, SEC (2012) 73 final. All documents are available at <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm> accessed 6 June 2012.

5 Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 ('Directive 95/46/EC').

number of important changes and improvements which will be described here. These relate to the new legal basis, the choice of legal instruments, their scope of application, reinforcing the rights of data subjects, enhancing the responsibility of controllers and processors, facilitating international transfers of personal data, guaranteeing independent enforcement, and ensuring protection of personal data by police and criminal justice authorities.

A new legal basis

Both proposals, for the Regulation and for the Directive, are based on Article 16 of the Treaty on the Functioning of the European Union (TFEU). This Article, introduced by the Lisbon Treaty, is the new legal basis for the adoption of comprehensive data protection rules.

Article 16 (1) TFEU provides that 'everyone has the right to the protection of personal data concerning them'. Together with Article 8 (1) of the Charter of Fundamental Rights of the European Union ('the Charter'),[6] Article 16 (1) TFEU therefore guarantees the fundamental right to the protection of personal data applying to all Union policies.

Article 16 (2) TFEU now unifies and replaces the previous distinct legal bases for regulating the processing of personal data by Community institutions and bodies (former Article 286 EC), in the former 'first pillar' Community (based on former Article 95 EC) and in the former 'third pillar' (Articles 30 (1)(b), 34 (2)(b) EU). This provision therefore now allows for the adoption of rules relating to the protection of individuals with regard to the processing of personal data both by Union institutions, bodies, offices, and agencies, as well as by member states when carrying out activities which fall 'within the scope of Union law' and for rules relating to the free movement of such personal data, which includes personal data processed by member states authorities or private parties.

As the reference to 'Union law' in Article 16 (2) TFEU is not qualified in any way, this reference covers equally primary and secondary law of the Union. Moreover, there is no limitation of the type of 'activities' of member states which can be governed. In particular, unlike Article 51 (1) of the Charter, Article 16 (2) TFEU does not contain a reference to the 'implementation of EU law'. Accordingly, all personal data processing activities of member states in the area of EU law are covered regardless of whether they constitute an implementation of EU law or not. In particular, the processing of personal data by police authorities or judicial authorities in criminal matters equally falls within the scope of Union law for the purposes of Article 16 (2) TFEU.

The additional reference in the Regulation to Article 114 (1) TFEU is only necessary for amending Directive 2002/58/EC[7] (Article 89 of the proposed Regulation), to take account of the different legal nature of the proposed Regulation and to the extent necessary that that Directive also provides for the protection of the legitimate interests of subscribers who are legal persons.[8]

Choice of legal instruments

Article 16 (2) TFEU mandates the European legislators to adopt 'the rules relating to the protection of individuals with regard to the processing of personal data', without, however, specifying the type of legislative act to be chosen. As a consequence, in line with Article 289(1) TFEU on the ordinary legislative procedure, the rules can be laid down in a regulation, a directive, or a decision.

Directive 95/46/EC set a milestone in the history of the protection of personal data in the European Union. The Directive enshrines two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals (in particular, the fundamental right to data protection), and the achievement of the internal market—the free flow of personal data in this case. In order to achieve this, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data must be equivalent in all member states ensuring a high level of protection, as recognized in recitals 8 and 10 of Directive 95/46/EC. As a consequence, the harmonization of national data protection laws by Directive 95/46/EC is not limited to minimal harmonization but amounts to harmonization that is generally complete.[9] While Directive 95/46/EC includes rules with a degree of flexibility and, in many instances, leaves to the member states the task

6 [2010] OJ C 83/389.

7 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('Directive on privacy and electronic communications'), [2002] OJ L 201/37.

8 The substantive legal consequences of the new Regulation and of the new Directive for Directive 2002/58/EC will be the object of a review by the Commission, taking into account the result of the negotiations on the data protection reform proposals with the European Parliament and the Council.

9 CJEU C-101/01 *Bodil Lindqvist* [2003] ECR I-1297, paras 96, 97.

of deciding the details or choosing between options, it precludes additional requirements to the principles.[10]

Although the objective of Directive 95/46/EC was to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the data protection rules across member states. As a consequence, data controllers may have to deal with 27 different national data protection laws and requirements within the EU. The result is a fragmented legal environment which has created legal uncertainty and unequal protection for data subjects. This has caused unnecessary costs and administrative burdens for controllers, in particular for businesses operating across borders. This irregular protection constitutes a disincentive for enterprises and affects the competitiveness of European companies. At the same time, the fundamental right to the protection of personal data requires the same level of data protection for individuals throughout the Union. Additional common EU rules are therefore necessary to avoid the risk of different level of protection in the member states.

The General Data Protection Regulation

In order to build on the existing standards of Directive 95/46/EC and to remedy its shortcomings, the Commission considers a Regulation to be the most appropriate legal instrument to define the general framework for the protection of personal data in the Union: the direct applicability of a Regulation in accordance with Article 288 TFEU will reduce legal fragmentation, provide greater legal certainty, improve the protection of individuals, and contribute to the free flow of personal data within the Union.

A Regulation directly applicable in all member states puts an end to the cumulative and simultaneous application of different national data protection laws. This will lead to a net saving for companies of about €2.3 billion a year in terms of administrative burden alone. A member state has no power to apply a Regulation incompletely or to select only those provisions of which it approves; nor can it invoke provisions or practices of domestic law to preclude the mandatory application of a Regulation.[11]

The direct applicability of a Regulation does not entail, however, a prohibition for member states to adopt laws at national level. Although member states are not allowed to 'transpose' a Regulation, as this would put into question its direct applicability, there can be specific circumstances and cases where national law may specify the application of some elements of a Regulation, within the limits set by the Regulation itself. This can be the case where, for example, detailed sectoral laws with data protection provisions (eg in the area of public health or social security) in the member states incorporate some elements of EU Regulations for the sake of coherence and to make them comprehensible to the addressees of that sectoral legislation.[12]

The proposed General Data Protection Regulation even requires member states to enact supplementary legislation: Article 5(a) states that personal data must be processed 'lawfully'. Article 6 (3) further provides that the legal basis for any processing which is either necessary to comply with a legal obligation (Article 6 (1)(c)) or necessary for the performance of a task carried out in the public interest (Article 6 (1)(e)) must be laid down either in Union law, or in the law of the EU member state to which the controller is subject. This is in particular relevant for controllers in the public sector where data processing generally relies on a legal obligation; a task carried out in the public interest requires a legal base in the relevant sectoral law. Therefore, additional member state laws will be necessary in those sectors, in application and in conformity with the Regulation.

Moreover, the Regulation also obliges or allows member states to provide for specific rules ('empowerments'). Member states can in particular adopt specific rules in order to ensure the right to freedom of expression (Article 80) or for laying down rules regulating data processing in the employment context (Article 82). The Regulation is also not going to affect member states' press and libel laws, which have to set out the balance between the privacy rights of the individual recognized in Article 7 of the Charter and the right to freedom of expression and information established in Article 11 of the Charter.

A number of provisions in the Regulation also explicitly refer to member state law, for example the obligation to authorize profiling measures (Article 20 (2)(b)), the possible limitations of data subject's rights (Article 21), and to the processing of personal data concerning health (Article 81). In this regard, member states have

10 CJEU Joined Cases C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado* [2011] ECR I-00000, para. 35.

11 Klaus-Dieter Borchardt, *The ABC of European Union law* (European Union 2010) 89.

12 See CJEU Case 230/78 *SpA Eridania-Zuccherifici nazionali and SpA Società Italiana per l'Industria degli Zuccheri v Minister of Agriculture and Forestry, Minister for Industry, Trade and Craft Trades, and SpA Zuccherifici Meridionali* [1979] ECR 02749, paras 26 and 27.

therefore, within the limits of the Regulation, a clear room for manoeuvre to take into account their national, historical, and cultural specificities.

In certain areas, the Regulation even allows for the explicit possibility for member states to complement the Regulation. This concerns, for example, the national rules on freedom of information and public access to documents which have 'to be taken into account' when applying the provisions set out in the Regulation (see recital 18).

The Directive for competent police and judicial authorities in criminal matters

The protection of personal data processed by police and judicial authorities in criminal matters is currently principally covered by Framework Decision 2008/977/JHA.[13]

The entry into force of the Lisbon Treaty, and Article 16 TFEU as the new legal basis for EU data protection legislation, call for the establishment of a comprehensive data protection framework which also covers the processing by police and judicial criminal authorities.[14]

However, 'comprehensive framework' does not necessarily mean 'single framework'. With a separate instrument next to a Regulation, the choice being for a Directive, the Commission took into account that more flexibility for the police and judicial criminal authorities of member states was needed, thereby addressing the specific nature of these fields.[15]

However, on substance, the Directive echoes the same principles enshrined in the Regulation and pursues as well the twofold aim of ensuring high protection for individuals and laying the legal foundation for the unhindered exchange of necessary information, and effective cooperation between member states' competent authorities.

A major difference to the Framework Decision, however, is that the proposed Directive is not confined to only laying down minimal harmonization standards: it aims at achieving a 'comprehensive harmonisation' in this sector, ensuring the 'same level of protection for individuals throughout the Union'.[16]

The current Framework Decision provides for a low 'minimum' level of harmonization as it leaves important details exclusively to member states' national law. An example is the right to information of the data subject set out in Article 16 of the Framework Decision. It provides for the obligation of member states to inform the individual that their personal data are being collected or processed by competent authorities, but only 'in accordance with national law'; this therefore, effectively paves the way for 27 very different implementing laws. The proposed Directive follows a different approach: Article 11 not only lays down the obligation to inform the data subject but also requires member states to provide 'at least' a certain number of specific details to them. Only in that way will the data subject be in a position to learn of the existence of a processing operation and, where data are collected from him, be given accurate and relevant information in a harmonized way throughout the Union in all 27 member states.

The Framework Decision expressly allows member states to impose higher safeguards at national level than those established in the Framework Decision (Article 1 (5) of the Framework Decision). As a consequence, Article 12 of the Framework Decision requires that national processing restrictions in place in one member state have to be met by the other member states. Conversely, the proposed Directive does not contain a corresponding clause; Article 1 (2) (b) of the proposed Directive requires member states neither to restrict nor prohibit the exchange of personal data by competent authorities within the Union regarding the protection of individuals and to the processing of personal data (in line with Article 1 (2) of Directive 95/46/EC and Article 1 (3) of the proposed Regulation).

While the envisaged harmonization under the Directive is aimed at being 'comprehensive', it is not 'complete' in the way Directive 95/46/EC envisages it: this Directive leaves considerably more flexibility for member states. By its very nature, it is bound to the result achieved, but leaves national authorities to decide the choice of form and methods (Article 289 TFEU). At the same time, in accordance with the prin-

13 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L 350/60 ('Framework Decision').

14 Article 9 of Protocol 36 on Transitional provisions annexed to the Treaty of Lisbon provides that in the case of the existing former third pillar acquis, the principle is the preservation of all legal acts so long as they are not repealed, annulled, or amended. The Commission has no infringement powers in the case of former framework decisions and the Court of Justice of the EU has only limited competence (Article 10). However, Declaration 50 concerning Article 10 of the Protocol 36 attached to the Treaties invites the institutions, within their respective powers, to seek to adopt, in appropriate cases and as far as possible within the five-year transitional period, legal acts amending or replacing existing third pillar acts.

15 See Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, as annexed to the Final Act of the Intergovernmental Conference which adopted the Lisbon Treaty.

16 See proposed Directive, Explanatory memorandum, point 3.2; recital 12.

ciple of subsidiarity, the Directive only establishes the necessary general data protection principles and rules at Union level, yet their detailed implementation is left to member states, thus allowing each member state to choose the regime which corresponds best to its particular situation. By way of example, Article 17 of the Directive, read together with recital 82, makes clear that member states may implement the exercise of the rights of data subjects on information, access, rectification, erasure, and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure (and not only in a data protection act for this sector).

Scope of application

Both the Regulation and the Directive contain several clarifications on their respective scope.

Activities outside the scope of Union law

Both the Regulation and the Directive do not apply to processing activities falling 'outside the scope of Union law' (Article 2 (2)(a) Regulation, Article 2 (3)(a) Directive). As safeguarding 'national security' remains the sole responsibility of member states, in line with Article 4 (2) TEU, it is therefore cited in both Article 2 (2)(a) of the Regulation and Article 2 (3)(a) of the Directive as a case of such an activity outside the scope of Union law.

As held by the Court of Justice of the European Union (CJEU) in a number of cases,[17] the rules on the protection of individuals regarding the processing of personal data and the free movement of such data apply regardless of whether or not there is a cross-border dimension. On this basis, the Court held that the processing of personal data by a national court of auditors in the context of its activities under national law did not fall 'outside the scope of Community law', and therefore did not fall under the exception of Article 3 (2) of the Directive.[18] The CJEU reached the same result for the religious and charitable activities of a church,[19] and for the processing of personal data by public authorities for the purposes of the application of immigration law, and for statistical purposes.[20] Consequently, after the entry into force of the Lisbon Treaty, the expression 'within the scope of Union law' must be interpreted as excluding only those areas which do not fall within the competences of the Union, as is the case for the matters listed in Article 3 (2), first indent, of Directive 95/46/EC with respect to the competences of the Community.

Application to domestic processing

The Framework Decision in principle only applies to the cross-border exchange of personal data within the EU and not to domestic processing operations in the member states.[21] The Directive will replace the Framework Decision (Article 58). As the Directive aims at achieving greater harmonization of EU member states' rules on data protection in the area of police and criminal justice, it follows the approach of Directive 95/46/EC and of the proposed Regulation, therefore also applying to domestic processing operations. This is necessary as neither Article 8 of the Charter nor Article 16 TFEU make a distinction between domestic and cross-border processing operations, but refer to processing activities that fall within the scope of EU law and the free movement of personal data. Likewise, the Council of Europe Convention No. 108 simply applies to the 'automatic processing of personal data in the public and private sectors'.[22]

Moreover, the Commission's assessment has shown that the 'domestic v cross-border data' differentiation is an artificial distinction and—as confirmed by some member states during the Commission's consultations—may also create practical problems for law enforcement authorities: it is difficult for a police officer to distinguish between data of different 'origins' during an investigation and to apply different rules to such personal data. Moreover, it is not always foreseeable in advance that personal data collected by one member state will then be subject to cross-border exchange. Therefore, common rules covering both 'domestic' data processing and cross-border transmissions between member states are a precondition for the effective exchange of personal data and will enhance law enforcement cooperation.

17 See CJEU Joined Cases C-465/00, C-138/01, and C-139/01 *Rechnungshof* [2003] ECR I-04989, paras 41–43; Case C-376/98 *Germany v Parliament and Council* [2000] ECR I-08419, para. 85; Case C-491/01 *British American Tobacco and Imperial Tobacco* [2002] I-11453, para. 60.

18 CJEU, Joined cases C-465/00, C-138/01, and C-139/01 *Rechnungshof* [2003] ECR I-04989, paras 41–43.

19 CJEU Case C-101/01 *Lindqvist* [2003] ECR I-12971, para. 45.

20 CJEU Case C-542/06 *Huber* [2008] ECR I-9705, para. 45.

21 More precisely, the Framework Decision applies to personal data that are or have been transmitted or made available between member states or exchanged between member states and EU institutions or bodies (see Article 1(2)).

22 See Article 3 (1) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981 (ETS No 108).

Union institutions, bodies, offices, and agencies

Both the proposals for the Regulation and for the Directive are addressed to member states only, and therefore do not apply to the processing of personal data by the Union institutions, bodies, offices, and agencies, which will continue to apply Regulation (EC) No 45/2001.[23]

As regards the scope of Regulation (EC) 45/2001, after the entry into force of the Lisbon Treaty, the references to 'Community institutions and bodies' and to 'Community law' in Article 3 (1) of that Regulation must be interpreted as references to 'Union institutions, bodies, offices and agencies' and to 'Union law'. Thus, that Regulation now applies to the processing of personal data by all Union institutions and bodies insofar as such processing is carried out in the exercise of all activities or part of which fall within the scope of Union law. Accordingly, since the entry into force of the Lisbon Treaty, the powers of the European Data Protection Supervisor (EDPS) under Regulation (EC) 45/2001 relate to the processing of data by all EU institutions, bodies, offices, and agencies.[24]

Putting individuals in control of their personal data

In a recent survey,[25] more than two-thirds of Europeans—72 per cent—said they were concerned about how companies use their personal data. Worries about online privacy are one of the most frequent reasons people do not buy goods and services on the Internet. Therefore, a high level of data protection is also crucial to enhance trust in online services and to fulfil the potential of the digital economy, thereby encouraging economic growth and the competitiveness of EU industries.

The aim of the new legislative acts proposed by the Commission is to strengthen individual rights, by improving individuals' ability to control their data and by giving data subjects efficient and operational means to make sure they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively.

Improving individuals' ability to control their data

1. *Clarifying 'consent'.* In line with Article 8 (2) of the Charter, Directive 95/46/EC and the Regulation list the data subject's consent as one possible ground for lawful processing of personal data. 'Consent' is currently defined in Articles 2 (h) and 7 (a) of Directive 95/46/EC as 'any freely given specific and informed indication' of a data subject's wish to agree to the processing of his personal data. This agreement must be 'unambiguously' given in order to make the processing of personal data legitimate. National laws have transposed this concept quite differently. Consequently, national supervisory authorities apply different interpretations of consent and its modalities. In particular, the meaning of 'unambiguously' given consent is interpreted in a variable manner: in some member states consent has to be given 'expressly' and in some cases even in writing, while other member states and supervisory authorities also accept some forms of implied consent. The consequence is that today valid consent in one member state may not be legally valid in others, therefore creating uncertainty amongst controllers operating in several member states on whether a data processing operation is lawful or not.

In the proposed Regulation, this legal uncertainty is effectively remedied: the definition of 'the data subject's consent' of Article 4 (8) adds the criterion 'explicit' to avoid the confusing parallelism with 'unambiguous' consent in addition to having one single and consistent definition of consent. Consent can be based either on a statement or on a clear affirmative action by the person concerned when freely given. Silence or inactivity therefore cannot constitute valid consent.

Where consent is the legal ground for data processing, Article 7 provides additional clarifications; in particular the controller must be able to demonstrate that consent has taken place. Moreover, the Regulation reaffirms that the data subject may withdraw his or her consent at any time; however, this will only take full legal effect for future processing.

Furthermore, the context of the consent should allow a genuine and free choice of the data subject: as a consequence, consent is excluded in Article 7 (4) as a ground for processing in specific cases of significant imbalance between data controller and data subject, for example in the framework of an employment relationship. Similarly, Article 8 sets out further conditions for the lawfulness of consent for the processing of personal data of children below the age of 13 years in

23 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 008/1.

24 However, EU legislation containing specific data protection rules applying to bodies established under the former third pillar, such as the rules established for Europol by Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) [2009] OJ L 121/37, take precedence over Regulation (EC) 45/2001 since they can be considered *lex specialis* vis-à-vis the latter.

25 SPECIAL EUROBAROMETER 359 *Attitudes on Data Protection and Electronic Identity in the European Union* <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf>.

relation to information society services offered directly to them.

2. *Introducing the 'right to be forgotten'.* The right to request from the controller the deletion of unlawfully processed personal data is already provided for by Directive 95/46/EC, but in the current practice it is difficult for an individual to enforce this right, especially in the online environment.

Therefore the new Regulation reinforces this current right. In particular, data subjects have, according to Article 17 (1)(a) to (d), the right to obtain from the controller that their personal data are deleted, and no longer processed should the personal data be no longer necessary in relation to the purposes for which it was collected or processed, where a data subject has withdrawn his consent for processing, where he objects to the processing of his personal data, or where the processing of his personal data otherwise does not comply with the Regulation.

Article 17 (1) makes equally clear that this right applies in particular in situations where a data subject has (validly) consented when he was a child, whilst not being fully aware of the risks involved by the envisaged processing. This person will now be able to remove any such personal data which were made public on the Internet at that time.

To further strengthen this 'right to be forgotten' in the online environment, the traditional right to erasure is extended in such a way that the controller who has made the personal data public is obliged to inform third parties processing the data that a data subject has requested the controller to erase any links to, or copies or replications of that personal data. To ensure this information of the third parties, the controller has to take 'all reasonable steps', including technical measures, taking due account of the controller's means—in relation to personal data for the publication of which the controller is responsible. In relation to the publication of personal data by a third party, and where the controller has authorized the publication by that third party, the controller can be held responsible for the publication (Article 17 (2)).

As underlined by the CJEU, the right to the protection of personal data, including the right to be forgotten, is not an absolute right, but must be considered in relation to its function in society.[26] The 'right to be forgotten' therefore cannot amount to a right of the total deletion of history. Neither can it take total precedence over the freedom of expression or freedom of the media. Accordingly, both situations figure amongst the exceptions to the right to erasure in Article 17 (3) and (4).

3. *Right to access and right to data portability.* Article 8 (2) of the Charter and Article 12 of Directive 95/46/EC already enshrine the right of access under data protection law: any person must be able to exercise his right of access to personal data relating to him, so that they can verify the accuracy of the data and the lawfulness of the processing.

The Commission considers that easier access to one's own personal data must be assured further, especially taking account of the vast amount of personal information processed today in online social networks. Therefore, Article 15 of the proposed Regulation on the data subject's right of access to their personal data builds on Article 12 (a) of Directive 95/46/EC; it also adds new elements, such as the controller's obligation to inform the data subjects about the envisaged or applied storage period, and of the rights to rectification, to erasure and to lodge a complaint with the competent supervisory authority.

While the right to access always includes the right to obtain communication of the actual data undergoing processing (Article 15 (2)), that is, a copy of all personal data processed by the controller in permanent form or on other types of media, the Regulation introduces a new right: the data subject's 'right to data portability'. Article 18 provides the right to obtain from the controller a copy of the personal data 'in a structured and commonly used electronic format', allowing for any further use by the data subject, in particular allowing the data subject to transfer this personal data from one automated processing system of the controller to and into another, without being prevented from doing so by the controller. This only applies, however, where the processing of the data subject's personal data in the system is based on his consent or in the performance of a contract, for example not in cases where the processing takes place based on a legal obligation. The general requirement for the controller to respond to requests of the data subject within a fixed deadline of a month (Article 12 (2)) also applies in these cases.

Improving the means for individuals to exercise their rights

Rights which cannot be enforced in practice are worthless. Where substantive EU rights are infringed, citizens and businesses must be able to enforce the rights granted to them by EU legislation. Under

26 CJEU, Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-0000, para. 48.

Directive 95/46/EC the ways in which individual data subjects may exercise their data protection rights are not sufficiently harmonized across member states. Nor are the powers of the national authorities responsible for data protection standardized enough to ensure consistent and effective application of the rules. This means that actually exercising such rights is more difficult in some member states than in others, particularly online.

As a consequence, the proposed Regulation is enhancing administrative and judicial remedies when data protection rights are violated. In particular, Article 76 (1) enables certain associations to be able to bring actions to court. As a precondition, in order to avoid from the outset the risk of abusive litigation, these data protection associations must act on behalf of one or a group of data subjects whose rights may have been violated, be sufficiently qualified, in particular by aiming at protection of data subjects' rights and interests as regards the protection of personal data, and be constituted as such according to the law of a member state (Article 73 (2)). Today, such associations already exist in some member states and could include, for example, consumer protection associations if their statutory aim includes the protection of personal data. Article 73 (3) provides in addition that these data protection associations may address a supervisory authority in any member state in cases of personal data breaches as defined in Article 4 (9) in their own right, that is without having to rely on a data subject's authorization to act on his behalf.

Enhancing the responsibility of controllers and processors

To enhance the Single Market dimension of personal data protection the Commission proposals for a directly applicable Regulation simplify the regulatory environment for controllers and processors alike by replacing 27 national data protection laws. The Regulation also proposes to drastically cut red tape and to do away with formalities such as the general notifications to supervisory authorities currently required by Article 18 of Directive 95/46/EC. This should lead to net savings of €130 million a year alone.

Such measures, however, may never lead to a lower level of protection, or lesser compliance with the law, to the detriment of the data subject. As an incentive for better compliance from the start, and an important compensatory measure, the Regulation establishes a general 'principle of responsibility' which takes account of the data protection debate on an 'accountability principle' and provides an insight into the EU's understanding of what is expected from those processing personal data.

Article 22 describes in detail the controller's obligation of responsibility: a controller must be able to 'demonstrate' compliance with the Regulation, including by way of adoption of internal policies and effective mechanisms for ensuring such compliance. The effectiveness of the controller's measures must be verifiable by internal or external data protection specialists (Article 22 (3)), or can be achieved by the data protection certification mechanisms envisaged under Article 39.

In order to effectively implement the data minimization principle contained in Article 5 (c), the Regulation sets out further obligations for the controller by requiring him to apply the principles of 'data protection by design' and 'data protection by default' (Article 23).[27] Data protection by default should be applied so that the most data protection friendly option is provided to the data subject as a default configuration. This includes a specific obligation to prevent personal data being made accessible by default to the public or to anyone not authorized to process such data.

Furthermore, the Regulation introduces a general mandatory notification of personal data breaches to both data protection authorities (where feasible, within 24 hours, Article 31 (1)) and the individuals concerned (Article 32) as an incentive for better data security. These measures build on the same concept as contained in Article 4 (3) of Directive 2002/58/EC as amended by Directive 2009/136/EC.[28]

So as to avoid data protection violations from the beginning, the Regulation introduces a specific obligation to carry out 'Data protection impact assessments' for organizations (controllers and processors alike) involved in risky processing (Article 33). Where for example, a controller wishes to process genetic data in large scale filing systems, he is required to evaluate the risks inherent to the processing and implement measures to mitigate those risks. This might require the involvement of the supervisory authority, in line with Article 34 (2)(a).

27 For the application of these principles in the field of energy supply and energy consumption, see Commission Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems [2012] OJ L 73/9.

28 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11.

Experience from member states has shown that data protection officers are good for business. The success of the mandatory introduction of data protection officers in Germany, together with their increasing numbers over the past few years in other member states, has also contributed to the development of sector-specific best practices in data processing and data protection.[29] As a consequence, the Regulation now requires controllers to designate a data protection officer in public authorities and in those companies with more than 250 employees or which are involved in processing operations which, by virtue of their nature, their scope, or their purposes, require a higher degree of compliance awareness and knowledge of the law (Article 35).

Facilitating international transfers of personal data

To address the challenges of globalization, flexible tools and mechanisms to facilitate international transfers of personal data in and outside of the European Union are needed—particularly for businesses operating worldwide—while guaranteeing the protection of individuals' data without any loopholes.

The Regulation lays down clear rules defining when its provisions apply to data controllers established in third countries, in particular whenever goods and services are offered to individuals in the EU, or whenever the behaviour of such individuals is monitored (Article 3(2)).

Legitimate flows of personal data from the EU to third countries are made easier by reinforcing and simplifying the rules on international transfers (Articles 40 to 44), including to those countries not subject to a Commission adequacy decision. This is achieved by streamlining and extending the use of tools such as Binding Corporate Rules (Article 43), so that these can be authorized by a supervisory authority to cover data processors and be applied within groups of companies too, thus better reflecting the increasing number of companies involved in data processing activities.

Article 45 of the Regulation explicitly provides for international cooperation mechanisms for the protection of personal data between the Commission and the supervisory authorities of third countries, in particular those considered to be offering an adequate level of protection. This provision takes into account the Recommendation of 12 June 2007 by the Organisation for Economic Co-operation and Development (OECD) on cross-border cooperation in the enforcement of laws protecting privacy.

Guaranteeing independent and consistent enforcement

Both Article 8 of the Charter and Article 16 (2) TFEU require independent authorities to check that the rules for the processing of personal data are complied with.

However, the status of independence, the resources and the powers of the national authorities responsible for data protection vary considerably among member states.[30] In some cases, they are unable to perform their enforcement tasks in a satisfactory way. Cooperation among these authorities at European level—especially via the existing Advisory Group (the so-called Article 29 Working Party)[31]—has not always led to consistent enforcement in the past.

As a consequence, the proposed Regulation further enhances the independence and powers of national data protection supervisory authorities to enable them to carry out investigations, take binding decisions and impose effective and dissuasive sanctions. In particular, Articles 46 to 50 now clarify in more detail the conditions for the establishment and for ensuring the complete independence of supervisory authorities in member states, taking inspiration from the relevant provisions in Regulation (EC) No 45/2001 and implementing the requirements by the Court of Justice of the European Union.[32] This includes obliging member states to provide them with sufficient resources.

Furthermore, the Regulation provides for fully harmonized provisions for the competences, duties, and powers of the supervisory authorities (Articles 51 to 54). It also creates the legal basis and the conditions for swift and efficient cooperation between supervisory authorities, including the obligation for one supervisory authority to carry out investigations and inspections upon request from another supervisory authority, and to mutually recognize each other's decisions (Articles 55 and 56).

Crucially, the Regulation provides in Article 51 that where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one

29 See a comparative analysis by the Confederation of European Data Protection Organisations (CEDPO): <www.cedpo.eu>.

30 For more details on this aspect, see the Impact Assessment accompanying the legal proposals, SEC (2012) 72.

31 The 'Article 29 Working Party' was set up in 1996 (by Article 29 of Directive 95/46/EC) with advisory status to the EU Commission and is composed of representatives of national Data Protection Supervisory Authorities, the European Data Protection Supervisor and the Commission. See <http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm>.

32 CJEU C-518/07 *Commission v Germany* [2010] ECR I-01885.

member state, only one single supervisory authority is competent for monitoring the activities of the controller or processor throughout the Union and for taking the related decisions. This 'one-stop-shop' should increase the consistent application of the EU's data protection rules, provide for greater legal certainty and reduce the administrative burden for companies. The competent authority for the one-stop-shop is the supervisory authority of the member state in which the controller or processor has its main establishment, as defined in Article 4 (13).

The Regulation sets up a novel consistency mechanism at EU level (Articles 57 to 63) to ensure that those supervisory authorities whose decisions may have a wider European impact can take full account of the views of other supervisory authorities concerned, and ensure compliance with EU law.

Finally, the Article 29 Working Party is renamed and transformed into an independent European Data Protection Board, to improve its contribution to the consistent application of data protection law and to provide a strong basis for cooperation among data protection authorities, including the European Data Protection Supervisor. Relationships should be forged by foreseeing that the secretariat of the European Data Protection Board will be provided by the European Data Protection Supervisor (Articles 64 to 71).

Ensuring protection of personal data by police and criminal justice authorities

In comparison with the current Framework Decision, the new Data Protection Directive that the Commission proposed for competent police and criminal justice authorities of member states includes improvements and new elements for achieving further harmonization and better protection of individuals: apart from the application to all domestic processing operations by competent authorities, the Directive requires member states to distinguish between different categories of data subjects (eg between convicted criminals and victims) (Article 5), and to distinguish personal data depending on their degree of accuracy and reliability (Article 6); it makes a crucial difference if personal data on an individual are stored by the police based on hearsay only or when based on a final court conviction.

The Directive equally harmonizes possible limitations of the individual's right of access, with the right of the data protection supervisory authority to check on the lawfulness of the processing even if the access right has been initially refused (Article 12 to 14).

Other improvements include the explicit introduction for police and criminal justice authorities of the obligation to implement the principles of data protection by design and data protection by default (Article 19), as well as to notify personal data breach notifications (Articles 28 and 29) and to designate data protection officers (Articles 30 to 32).

A transfer of personal data to a third country or an international organization by police and criminal justice authorities may now take place when the Commission has decided that the third country in question ensures an adequate level of protection, either based on Article 41 of the Regulation or by adopting a sector-specific decision under the Directive Article 34 (3). As is the case already today, when a third country has been found to be adequate by the Commission, data transfers to that third country do not require any national authorization.

The Directive provides for the legal base for the mutual assistance of supervisory authorities (Article 48) and acknowledges an explicit competence of the European Data Protection Board for this Directive (Article 49).

The next steps

The EU data protection reform aims to build a modern, strong, consistent, and comprehensive data protection framework for the European Union. Individuals' fundamental right to data protection are reinforced. Other rights, such as the freedom of expression and information, the rights of the child, or the right to conduct a business are respected.

A strong, clear and uniform legislative framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation, and job creation, in line with the objectives of the EU's growth strategy Europe 2020[33] and the Digital Agenda for Europe:[34] the Regulation will do away with the patchwork of legal regimes across the 27 member states and remove barriers to market entry, a factor of particular importance to micro, small, and medium-sized enterprises. National supervisory authorities are reinforced and their cooperation strengthened to guarantee the consistent enforcement and, ultimately,

33 Communication from the Commission 'EUROPE 2020 A strategy for smart, sustainable and inclusive growth' COM (2010) 2020 final.

34 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions 'A Digital Agenda for Europe' COM (2010) 245 final/2.

uniform application of the data protection rules across the EU.

The new rules also give EU companies an advantage in global competition. Under the reformed regulatory framework, they will be able to assure their customers that valuable personal data will be treated with the necessary care and diligence. Trust in a coherent EU regulatory regime will be a key asset for service providers and an incentive for investors looking for optimal conditions when locating services. Equally, the reform will enhance trust amongst member states' law enforcement authorities, facilitating exchanges of personal data between them and cooperation in the fight against crime, while ensuring a high level of protection for individuals.

The Commission's proposals have already sparked favourable opinions from the data protection community across Europe, in particular the Article 29 Working Party and the European Data Protection Supervisor.[35]

The European Commission is now working closely with the European Parliament and the Council to ensure an agreement on the EU's new data protection framework in the year 2013.

doi:10.1093/idpl/ips015
Advance Access Publication 25 June 2012

35 See, in particular, Article 29 Working Party, 'Opinion 1/2012 on the data protection reform proposals' (WP 191, of 23 March 2012); European Data Protection Supervisor, 'Opinion on the data protection reform package', of 7 March 2012.