"EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation"

Peter Hustinx[*]

1. Introduction

The concept of 'data protection' was developed almost four decades ago in order to provide legal protection to individuals against the inappropriate use of information technology for processing information relating to them. It was not designed to *prevent* the processing of such information or to *limit* the use of information technology per se. Instead, it was designed to provide safeguards whenever information technology would be used for processing information relating to individuals. This was based on the early conviction that the extensive use of information technology for this purpose could have far reaching effects for the rights and interests of individuals.[1]

In other words, data protection was about the rights and interests of individuals and - in spite of the terminology used - not mainly about the data relating to those individuals. In any case, the concept was invented at a point in time when the ubiquitous use of information technology was still in its early days. That is quite different now and the potential impact of such use is - due to the Internet and mobile devices - now all around us, every minute of every day, both in our personal and in our professional lives. This situation is likely to increase even further in the future. It is therefore appropriate to consider the current state of EU data protection law in the context of a course on EU law and technology.

Another reason for the relevance of EU data protection law is that its current main instrument - Directive 95/46/EC, also known as the Data Protection Directive - is now the subject of a wide ranging review to make it more effective in a world where information technology is playing a prominent role in all fields of life - both public and private. This review is approaching the final stage of political decision making: the European Parliament and the Council are preparing for negotiations to establish the future EU legal framework for data protection, possibly even for a few decades. For this reason, it is also the right moment to

---

[*] European Data Protection Supervisor (2004-2014). This article is based on a course given at the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013. It also draws on material used in multiple articles and speeches published by the author during recent years, such as P.J. Hustinx, 'Gegevensbescherming in de informatiemaatschappij', in E.J. Numan et al. (ed.), *Massificatie in het privaatrecht* (2010), at 77-91, and P. Hustinx, 'EU Data Protection Law - Current State and Future Perspectives', speech at High Level Conference: 'Ethical Dimensions of Data Protection and Privacy', Centre for Ethics, University of Tartu / Data Protection Inspectorate, Tallinn, Estonia, 9 January 2013, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_EN.pdf (last accessed 31 May 2014). The author is grateful for comments made on a draft version by C. Docksey.

[1] See *infra* Section 2.

take stock of where we are in EU data protection law and to take a closer look at some of the key issues.[2]

The context of the review only adds to the relevance of this exercise. Apart from the dynamic character of our digital environment and the ambition to benefit from these developments in a Digital Agenda that contributes to economic growth, we have recently also discovered that this environment is more vulnerable than most people had assumed. The revelations of large scale monitoring of our online behaviour by the US National Security Agency and other intelligence services have rightly sent shock waves around the world. At the same time, it is now clear that many business practices on line, including some of the most popular ones, are also based on extensive monitoring of consumer behaviour, and that the growing practice of providing 'free' services in exchange for monitoring has created opportunities for large scale spying by other actors. The review of the EU legal framework for data protection is therefore taking place in a context where both the need for more effective protection and the challenges to deliver that protection in practice have increased enormously. Although we will not be able to answer all relevant questions, it would still be useful to consider some of the solutions that are being developed to address those challenges.

In this article we will also look at the origins of EU data protection law and the distinctions between 'privacy' and 'data protection' that have contributed to its further development. It is necessary to better understand these points so as to appreciate the issues that may arise in the context of the present and the future legal frameworks. There are also important connections between both concepts. Privacy and data protection - more precisely: the right to *respect* for private life and the right to the *protection* of someone's personal data - are both fairly recent expressions of a universal idea with quite strong ethical dimensions: the dignity, autonomy and *unique value* of every human being. This also implies the right of every individual to develop their own personality and to have a fair say on matters that may have a direct impact on them. It explains two features that frequently appear in this context: the need to prevent undue *interference* in private matters, and the need to ensure adequate *control* for individuals over matters that may affect them.

Privacy and data protection as a specific field of law have developed over the last four decades at European level, notably first in the context of the Council of Europe, and at a later stage mainly in the context of the European Union. However, as the EU has continued on the basis of the work done in the Council of Europe, we will have to look at both in order to get a complete picture. In this overview we will see two main lines: the first one having to do with the development of *stronger* privacy and data protection rights as such, and the second with the need to ensure a *more consistent* application of those rights across the EU. Both are aiming to promote *more effective* protection in practice and less *unhelpful diversity* in the way

[2] See *infra* notably Sections 5-7.

protection is delivered in the Member States. In both lines we will see a gradual development in different stages, which now also involves the increasing impact of the Charter of Fundamental Rights, both in the case law of the Court of Justice and in the review of the current legal framework. As 'privacy' and 'data protection' are mentioned separately in the Charter, this also leads to issues as to the distinction between the two.

This article will largely follow the historic timeline: the origins of data protection and the role of the Council of Europe will be discussed in Section 2 and the main lines of the current EU Directive in Section 3. After an intermezzo in Section 4 on different institutional aspects, including the Charter and the impact of the Lisbon Treaty, we will turn to the background and the main lines of the proposed General Data Protection Regulation in Section 5. In Section 6 we will highlight some of the key issues in the current legislative debate and in Section 7 we will address other issues which may require further reflection and discussion. Finally, we will make some concluding remarks in Section 8.

2. The Origins of Data Protection

A. Privacy and Private Life

It was only after the Second World War that the concept of a 'right to privacy' emerged in international law. This first arose in a rather weak version in Article 12 of the Universal Declaration of Human Rights[3], according to which no one shall be subjected to *arbitrary* interference with his privacy, family, home or correspondence.

A more substantive protection followed in Article 8 of the European Convention on Human Rights (ECHR)[4], according to which everyone has the right to *respect* for his private and family life, his home and his correspondence, and no interference by a public authority with the exercise of this right is allowed except in accordance with the law and where necessary in a democratic society for certain important and legitimate interests.

The mentioning of 'home' and 'correspondence' could build on constitutional traditions in many countries around the world, as a common heritage of a long development, sometimes during many centuries, but the focus on 'privacy' and 'private life' was new, and an obvious reaction to what had happened in the Second World War.

The scope and consequences of this protection have been explained by the European Court of Human Rights in a series of judgments.[5] In all these cases, the Court considers - briefly put - whether there was an *interference* with the right to respect for private life, and if so whether it

[3] UN General Assembly, Paris 1948
[4] Council of Europe, Rome 1950
[5] See e.g. *infra* Section 2, Part D

had an *adequate* legal basis - i.e. clear, accessible and foreseeable - and whether it was *necessary* and proportionate for the legitimate interests at stake.

B. Data Protection

In the early 1970's the Council of Europe concluded that Article 8 ECHR had a number of shortcomings in the light of new developments, particularly in view of the growing use of information technology: the uncertainty as to what was covered by 'private life', the emphasis on protection against interference by 'public authorities', and the lack of a more pro-active approach, also dealing with the possible misuse of personal information by companies or other relevant organisations in the private sector.[6]

This resulted in two recommendations of the Committee of Ministers to the Member States to take all necessary steps to give effect to certain principles on the protection of the privacy of individuals in the private and the public sector.[7] This coincided with the first initiatives at national level in countries such as Germany and Sweden.[8]

The positive experiences with these first initiatives worked as a stimulus for the Council of Europe to invest time in the preparation of an international agreement as the first binding instrument on the subject. After four years this resulted in the adoption of the Data Protection Convention, also known as Convention 108[9], which has now been ratified by 46 countries, including all EU Member States, most Member States of the Council of Europe and one non-Member State.[10]

The purpose of the Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection').[11] The concept of 'personal data' is defined as 'any information relating to an identified or identifiable individual ('data subject')'.[12]

---

[6] Explanatory Report to Convention 108 (see below footnote 9), para. 4

[7] Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector, and Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector.

[8] The first national law was adopted in Sweden in 1972. The German State of Hessen adopted the world's first law on data protection in 1971. The United States also played a leading role at that stage with the formulation of 'fair information principles' which had a great influence on the international debate. See the report '*Records, Computers and the Rights of Citizens'*, US Department of Health, Education and Welfare, 1973, and the Privacy Act adopted in 1974.

[9] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108.

[10] Uruguay was the first non-Member State to ratify the Convention in April 2013.

[11] Article 1

[12] Article 2 sub a

This means that 'data protection' is *broader* than 'privacy protection' because it also concerns other fundamental rights and freedoms, and all kinds of data *regardless* of their relationship with privacy, and at the same time *more limited* because it merely concerns the processing of personal information, with other aspects of privacy protection being disregarded.

In this context, it should be noted that many activities in the public or the private sector are nowadays connected, in one way or another, with the collection and processing of personal information. The real objective of the Convention is therefore to protect individuals (citizens, consumers, workers, etc.) against unjustified collection, recording, use and dissemination of their personal details. This may also concern their participation in social relations, whether or not in public, and involve protecting freedom of expression, preventing unfair discrimination and promoting 'fair play' in decision-making processes. Finally the Convention also aimed to reconcile the respect for privacy and the free flow of information.[13]

C. Structural Safeguards

The Convention contains a number of basic principles for data protection to which each Party must give effect in its domestic law before it enters into force in respect of that Party.[14] These principles still form the core of any national legislation in this area. According to the Convention, personal data are to be 'obtained and processed fairly and lawfully' and 'stored for specified and legitimate purposes and not used in a way incompatible with those purposes', as well as 'preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored'. Personal data should also be 'adequate, relevant and not excessive in relation to the purposes for which they are stored' and 'accurate and, where necessary, kept up to date'.[15]

The Convention provides for stricter conditions as to 'special categories of data'.[16] Under this provision 'personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life' may not be processed, unless domestic law provides appropriate safeguards. The same applies to personal data relating to criminal convictions.

Other basic principles of the Convention call for 'appropriate security measures'[17] and 'additional safeguards for the data subject' such as the right to have access to his or her own personal data, the right to obtain, as the case may be, rectification or erasure of such data, and the right to remedy if such rights are not respected.[18] The concept of 'independent

[13] Preamble, para. 4
[14] Article 4
[15] Article 5
[16] Article 6
[17] Article 7
[18] Article 8

supervision' was initially not incorporated in the Convention, but nevertheless followed widely in practice and at a later stage added to the Convention via a Protocol.[19]

To be clear: the Convention's approach is *not* that processing of personal data should always be considered as an *interference* with the right to privacy, but rather that for the *protection* of privacy and other fundamental rights and freedoms, any processing of personal data must *always* observe certain legal conditions. Such as the principle that personal data may only be processed for specified legitimate purposes, where necessary for these purposes, and not used in a way incompatible with those purposes.

Under this approach, the core elements of Article 8 ECHR, such as interference with the right to privacy only on an adequate legal basis, and where required for a legitimate purpose, have been transferred into a broader context. In addition, under the Convention, no exceptions to these principles are allowed, except under similar conditions as for the right to privacy itself.[20]

It should be clear that this only works well in practice, if the system of checks and balances, set out in the Convention - consisting of substantive conditions, individual rights, procedural provisions and independent supervision - is sufficiently flexible to take account of variable contexts, and is applied with pragmatism and an open eye for the interests of data subjects and other relevant stakeholders. In this approach, the right to respect for private life set out in Article 8 ECHR continues to play an important role in the background, *inter alia* to determine the legitimacy of specific, more intrusive measures.

The Convention has played a major role in most Member States of the Council of Europe in setting out legislative policy. In this context, the issue of 'data protection' has been regarded from the outset as a matter of great structural importance for a modern society, in which the processing of personal data is assuming an increasingly important role. The Convention is currently also under revision and we will briefly return to this theme at a later stage.

D. Other Aspects

After the adoption of Convention 108, the Council of Europe continued to play an active role in the development of a series of recommendations of the Committee of Ministers about its application in different sectors. This resulted in important clarifications of some of the key

[19] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001; see notably Article 1. This was mainly due to the relevant provisions in Directive 95/46/EC (see infra Section 3, Part B).

[20] Article 9

provisions.[21] These recommendations have prepared the way for national legislation and also provided useful benchmarks for other international agreements.[22]

The provisions of the Convention were not intended to be directly applicable or included in judicial supervision of the ECHR. However, since 1997 the European Court of Human Rights has ruled in a number of cases that the protection of personal data is of 'fundamental importance' for a person's enjoyment of the right to respect for private life under Article 8 ECHR, and has derived yardsticks from the Convention for determining the extent to which that right had been infringed.[23] This suggests that the Court is increasingly inclined to assess compliance with the Convention - at any rate for 'sensitive data' - within the context of Article 8 ECHR.

This also leads to the question to what extent the shortcomings of Article 8 ECHR which led to the adoption of Convention 108 still exist. The concept of 'private life' in Article 8 is still not entirely clear, but its scope has increased considerably.[24] According to the case law of the Court, it is not limited to 'intimate' situations, but also covers certain aspects of professional life and behaviour in public, either or not in the past. On the other hand, those cases still often concern specific situations, which involve sensitive information (medical or social services), justified expectations of privacy (confidential use of telephone or email at work) or inquiries by police or secret services. The Court has so far never ruled that *any* processing of personal data - *regardless* of its nature or context - falls within the scope of Article 8.[25] The Convention therefore merely serves as an additional source of standards for the assessment of conduct within the scope of that provision.

---

[21] For instance, Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics, clarified the concept of 'personal data' in point 1.2 stating that an individual should not be regarded as 'identifiable' if the identification requires 'an unreasonable amount of time, cost and manpower'. The explanatory report to the Convention had said rather ambiguously that an 'identifiable person' was a person who could be 'easily identified: it does not cover identification of persons by means of very sophisticated methods' (para. 28).

[22] Recommendation No. (87) 15 on the use of personal data in the police sector has served as a benchmark for the level of data protection with regard to Europol (see Article 14 of the Convention based on Article K.3 of the EU Treaty on the establishment of a European Police Office (Europol Convention) and recital 14 of the current Europol Council Decision 2009/371/JHA).

[23] See e.g. *Z v Finland*, Application 22009/93, ECHR 1997-I, at 95.

[24] See e.g. *Klass v Germany*, ECHR (1978), A-28; *Malone v United Kingdom*, ECHR (1984), A-82; *Leander v Sweden*, ECHR (1987), A-116; *Gaskin v United Kingdom*, ECHR (1989), A-160; *Niemietz v Germany*, ECHR (1992), A-251-B; *Halford v United Kingdom*, ECHR 1997-IV; *Amann v Switzerland*, ECHR 2000-II, and *Rotaru v Romania*, ECHR 2000-V.

[25] In spite of sometimes ambiguous language, e.g. in *Khelili v Switzerland*, 18.10.2011, Application 16188/07, at 56: 'The storage of data *concerning the applicant's private life*, including her profession, and the retention thereof, amounted to an interference within the meaning of Article 8, *because it was personal data relating to an identified or identifiable individual*' (emphasis added). However, the case was about the conservation of data, including a reference to the applicant as a prostitute, for a long period by the police, without a sufficient factual basis. Moreover, in the same judgment, the Court also said that whether the conservation of personal data raises any aspect of private life depends on the particular context in which these data have been collected and retained, the nature of the relevant data, the way in which they are used and processed, and the consequences this may have (see at 55).

The Court has now also ruled that Article 8 ECHR may give rise to positive obligations for the Member States and that they may thus be held liable for a breach of privacy committed by a private party.[26] However, the number of relevant cases is still limited and does not amount to a general obligation for the Member States to ensure protection of personal data in horizontal relations. The Convention therefore continues to play a useful complementary role in this respect.

Only a few years after Convention 108 had been adopted, the German Constitutional Court delivered a decision in which it formulated a right to 'informational self-determination' as an expression of the right to free development of the personality as laid down in Article 2(1) of the German Constitution.[27] In this approach, any processing of personal data is in principle regarded as an interference with the right to informational self-determination, unless the data subject has consented. This decision has been very influential, not only in Germany, but also elsewhere in Europe. However, it should be clearly distinguished from the approach followed in Convention 108, and on that basis - as we will see - in Directive 95/46/EC and the relevant provisions of the EU Charter.

A few months before Convention 108 was adopted, the OECD adopted Privacy Guidelines which, although not-binding, have also been very influential, particularly in countries outside Europe, such as the United States, Canada, Australia and Japan.[28] The Guidelines contained a set of basic principles drawn up in close coordination with the Council of Europe and were therefore consistent with the principles for data protection in Convention 108. However, there were also quite subtle, but meaningful differences in details. The scope of the Guidelines was limited to personal data 'which because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.'[29] This implied the notion of 'risk' as a *threshold* condition for protection which was not entirely compatible with the fundamental rights based approach of the Council or Europe. Moreover, the need for a *legitimate* purpose and a *lawful* basis for processing of personal data per se was absent in the Guidelines.[30] Both points relate to issues which are still highly relevant in global discussions.

---

[26] See e.g. *von Hannover v Germany*, ECHR 2004-VI, and *K.U. v Finland*, Application 2872/02, ECHR 2008-V.
[27] Judgment of 15 December 1983, BVerfGE 65, 1-71, *Volkszählung.*
[28] OECD Council Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, Paris, 23 September 1980, available at: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 31 May 2014)
[29] Guidelines, para. 2
[30] See Guidelines, para. 7: '... data should be obtained by *lawful and fair means* and, *where appropriate*, with the knowledge or consent of the data subject.' (emphasis added)

3. Directive 95/46/EC

A. Harmonisation

Although the Council of Europe was very successful in putting 'data protection' on the agenda and setting out the main elements of a legal framework, it was less successful in terms of ensuring sufficient consistency across its Member States. Some Member States were late in implementing Convention 108, and those who did so arrived at rather different outcomes, in some cases even imposing restrictions on data flows to other Member States.

The European Commission was therefore quite concerned that this lack of consistency could hamper the development of the internal market in a range of areas - involving free circulation of people and services - where the processing of personal data was to play an increasingly important role. At the end of 1990, it therefore submitted a proposal for a Directive in order to harmonise the national laws on data protection in the private and most parts of the public sector. [31]

After four years of negotiation, this resulted in the adoption of the current Directive 95/46/EC[32] which has a double objective. Firstly, it requires all Member States to protect the fundamental rights and freedoms of natural persons, and in particular the right to privacy with respect to the processing of personal data, in accordance with the Directive. Secondly, it requires them neither to restrict, nor to prohibit the free flow of personal data between Member States for reasons connected with such protection.[33] Both obligations are closely interrelated. They aimed to bring about an equivalent high level of protection in all Member States with a view to achieving a balanced development of the internal market.

In that respect, the Directive started from the basic principles of data protection, as set out in Convention 108 of the Council of Europe.[34] At the same time, it specified those principles and supplemented them with further requirements and conditions. However, since the Directive adopted generally formulated concepts and open standards, it still allowed Member States fairly broad discretion on its transposition.[35] The result is that the Directive has led to a much greater consistency between Member States, but certainly not to identical or fully consistent solutions.

---

[31] COM (90) 314 final - SYN 287 and 288, 13 September 1990, page 4: 'The diversity of national approaches and the lack of a system of protection at Community level are an obstacle to completion of the internal market. If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross-border flow of data might be impeded...'

[32] Directive 95/46/EC 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, OJ L 281, 23.11.95, p. 31.

[33] See Recitals 7-10 and Article 1.

[34] See notably Recital 11.

[35] See Recital 9 and Article 5

B. Scope and Substance

The current Directive has a broad scope: it applies to all processing of personal data wholly or partially by automatic means, and to the processing by other means of personal data in or intended for a filing system[36] There are two exceptions: first, processing outside the scope of Community, now Union, law and in any event where it concerns public security, defence, state security or criminal law enforcement, and second processing by a natural person in the course of a purely personal or household activity.[37] The definitions of terms like 'processing' and 'personal data' are very close to those in Convention 108.[38]

The Directive also follows the basic principles for data protection set out in the Convention, but includes six criteria for the legitimacy of data processing which are not specified in the Convention.[39] In this respect, personal data may be processed only if the data subject has *unambiguously consented,* or if processing is *necessary* for the performance of a contract to which the data subject is party, for compliance with a legal obligation, for the performance of a government task, to protect the vital interests of the data subject, or to protect the legitimate interests of the controller, except where such interests are overridden by the interests of the data subject. This requires a subtle examination of the different phases of data processing and makes it necessary for data controllers to take this analysis into account at the right time.

The Directive also specifies the conditions for the processing of special categories of sensitive data.[40] The starting point is a *prohibition* with certain exceptions: either an *explicit* consent of the data subject, or compliance with specific conditions, such as for the use of health data in health care. Other exceptions can be made at national level, but only for reasons of 'substantial public interest' and 'subject to suitable safeguards'. The Directive provides for a notification to the Commission to ensure the restrictive use of this option.

Another feature of the Directive is the obligation for the controller to provide the data subject with adequate information, except where he already has it, on its identity, the purposes of the processing and other relevant matters, in so far as such further information is 'necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair

[36] Article 3(1)
[37] Article 3(2)
[38] Article 2 sub (a) and (b). See on the second subject in more detail: Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007 (WP 136), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (last accessed 31 May 2014).
[39] Article 7. See in this context Article 29 Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011 (WP 187) and Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014 (WP 217), available at:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (last accessed 31 May 2014)
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last accessed 31 May 2014)
[40] Article 8

processing' in respect of the data subject.[41] Failing to provide such transparency may lead to the data being obtained unlawfully, with all the relevant consequences.

The Directive also provides for the establishment of supervisory authorities for monitoring compliance with national legislation on their territory, with a number of specific functions and powers, which they must exercise 'with complete independence'.[42] These may involve prior checking or consultation[43], complaint handling, inspections, and other enforcement activities, depending on how the Directive has been implemented in national law. These authorities cooperate in the exercise of their functions, either bilaterally or in the context of the 'Article 29 Working Party' with independent advisory status at EU level.[44]

The territorial scope of the Directive applies to the processing of personal data carried out 'in the context of the activities of an establishment' of the controller on the territory of an EU Member State.[45] The location where the data are processed is not relevant in this respect. This criterion is also decisive for the scope of national law within the EU. Where the controller is not established in the EU, the applicable law is that of the Member State where the means used for the processing are located.[46]

The Directive also applies the principle that personal data may only be transferred to third countries that ensure an adequate level of protection. In the absence of such protection, transfer is only permitted in certain situations, either on the basis of an exception, or where adequate safeguards have been provided in contracts or other relevant instruments.[47]

These provisions now apply to a complex reality in which, both within the EU and in relation to third countries, the question arises increasingly frequently as to what law applies and who is responsible for its compliance. This also raises new questions concerning the Internet - on the position of websites, search engines[48], social networks and modern advertising technology - and relating to data flows within multinational companies, outsourcing of services and cloud computing. In practice, adequate protection is increasingly frequently

[41] Articles 10-11
[42] Article 28
[43] Articles 18-20
[44] Articles 29-30 which also refer to the European Data Protection Supervisor as a member of this group.
[45] Article 4. See the CJEU in Case C-131/12, *Google Spain*, 13 May 2014, not yet published, at 55-56. See also *infra* Section 6, Part D
[46] See in more detail Article 29 Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010 (WP 179), available at:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf (last accessed 31 May 2014)
[47] Articles 25-26. On this basis the European Commission has recognised a number of third countries with an adequate level of protection, and approved contractual clauses which can provide adequate protection in specific cases. For further information, see website of the European Commission and the Article 29 Working Party:
http://ec.europa.eu/justice/data-protection/index_en.htm (last accessed 31 May 2014)
[48] See e.g. *Google Spain* (footnote 45), ruling that a search engine operator is a controller and has to ensure compliance with EU data protection law (see at 33 and 38). See also *infra* Section 6, Part D.

delivered in 'binding corporate rules', codes of conduct endorsed by enterprises that meet specific requirements and which competent supervisory bodies accept as sufficiently effective.[49]

The need to reconcile respect for privacy and the free flow of information - one of the aims of Convention 108 and also visible in the objectives of the Directive - finally resulted in a more specific provision requiring Member States to provide for potentially very broad exemptions or derogations from certain provisions for the processing of personal data 'carried out solely for journalistic purposes or the purpose of artistic or literary expression' where necessary to reconcile the right to privacy with the rules governing freedom of expression.[50]

C. Relevant Case Law

All EU Member States have transposed the Directive into national law, including the new Member States for which transposition was a condition of accession, as well as the non-EU parties to the EEA. The Commission has by now also launched several legal actions for improper implementation of the Directive. The first action involved the Member State with the longest experience in this area: Germany. In March 2010 the Court of Justice ruled that the requirement of 'complete independence' for a supervisory authority means that it should be free from *any* external influence.[51] This position has more recently been confirmed and elaborated in cases against Austria and Hungary.[52]

The Court of Justice has also issued important judgments on other aspects of the existing legal framework for the protection of personal data. In its first judgments on Directive 95/46/EC for example, the Court ruled that it has a very broad scope which is not dependent in each case on a direct link with the internal market.[53] This meant that the Directive also applies to a dispute in the public sector of a single Member State, or to the website of a church or charitable foundation. In the latter case, it also became clear that the Directive applies in principle to the Internet, although the mere fact that personal data are available on a website does not mean that the provisions governing data traffic with third countries apply.[54] The precise consequences of this conclusion are not yet entirely clear.

[49] Article 26(2) provides that adequate safeguards may 'in particular' result from appropriate contractual clauses, but does not exclude other instruments. Additional information on BCR is available on the website mentioned in footnote 44.
[50] Article 9
[51] Case C-518/07, *Commission v Germany*, [2010] ECR I-01885, at 30
[52] Case C-614/10, *Commission v Austria*, 16 October 2012, and Case C-288/12, *Commission v Hungary*, 8 April 2014, both not yet published.
[53] Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk*, [2003] ECR I-04989, at 41-43, and Case C-101/01, *Bodil Lindqvist*, [2003] ECR I-12971, at 39-41.
[54] *Bodil Lindqvist*, at 24-27 and 56-71.

Where the Directive applies to an area within the scope of Article 8 ECHR, it must be interpreted in accordance with that provision.[55] In that context, the Court distinguished between processing operations that may - or may not - breach Article 8 ECHR. The former applied to a national law compelling employers to supply certain salary data to a government body. Processing of the same data by the employer for employment purposes did not raise any issue of principle, as long as data protection rules were respected.[56] This fits well in the distinction between 'privacy' and 'data protection' in the development of the law, as referred to before.

The exception for data processing concerning public security and criminal law enforcement was applied by the Court in a major case about the transfer of airline passenger data to the US for the purpose of border protection following the terrorist attacks on 11 September 2001.[57] In other cases, the Court held that the exception for data processing by a natural person in the course of a purely personal or household activity only applies to activities which are carried out in the course of private or family life of individuals, which is clearly not the case where personal data are made accessible to an indefinite or unrestricted number of people.[58] In one of those cases, the Court also ruled that the exception for journalistic purposes should be applied broadly, so as to include all activities with the sole object to disclose information, opinions or ideas to the public.[59]

In a case about the criteria for legitimate data processing, the Court ruled that Spain had not transposed Article 7(f) of the Directive correctly, by requiring that - in the absence of the data subject's consent - any data processed should appear in public sources.[60] The Court also held that Article 7(f) has direct effect.[61] The judgment limits the margin of discretion that Member States have in implementing Article 7(f). In particular, they must not overstep the fine line between specification or clarification on the one hand, and imposing additional requirements, which would amend the scope of Article 7(f) on the other hand.

In a case on the scope of the right of access to automated population files in the Netherlands, the Court ruled that Member States are required to ensure a right of access to information on past processing, notably on the recipients of personal data and on the content of the data disclosed in the past. It is for Member States to fix a time-limit for storage of that information and to provide for access which constitutes a fair balance between, on the one hand, the

[55] *Österreichischer Rundfunk*, at 68-72
[56] *Österreichischer Rundfunk*, at 73-74
[57] Joined Cases C-317/04 and C-318/04, *PNR*, [2006] ECR I-04721, at 56-59 and 67-69. See for critical analysis of this judgment: C. Docksey, 'The European Court of Justice and the Decade of Surveillance', in H. Hijmans and H. Kranenborg (ed.), *Data Protection Anno 2014: How to Restore Trust?* (2014), at 97-111.
[58] *Bodil Lindqvist*, at 46-47, and Case C-73/07, *Satamedia*, [2008] ECR I-09831, at 43-44.
[59] *Satamedia*, at 56 and 61.
[60] Joined Cases C-468/10 and C-469/10, *ASNEF*, [2011] ECR I-12181, at 32-39 and 49.
[61] *ASNEF*, at 51-54.

interest of the data subject in protecting his privacy, and on the other, the burden which the obligation to store that information represents for the controller. However, rules limiting the storage of information on processing to one year, while the basic data themselves are stored for a much longer period, do not set a fair balance between the interest and obligation at issue, unless longer storage would put an excessive burden on the controller.[62] This ruling shows a sharp understanding of the key role of the data subject's right of access and the complex environment in which it may have to be exercised in practice.

4. Institutional Aspects

A. Other Instruments

So far we have focussed on Directive 95/46/EC, but this is not the only relevant instrument of EU data protection law. There are at least three other categories of instruments - namely acts specifying the rules in a particular area, applying the rules at EU level, and applying them in the law enforcement area - which should be mentioned briefly. An example of the first one is Directive 2002/58/EC on privacy and electronic communications, which specified Directive 95/46/EC in the area of publicly available electronic communications services and public communications networks.[63] It deals with issues ranging from security and confidentiality of communications to the storage and use of traffic and location data, and unsolicited communications, regardless of the technology used. Although the Directive therefore also applies to the Internet, it does so only within its own scope. Some important data processing around websites continues to fall under the scope of Directive 95/46/EC.[64]

An example of the second category is Regulation (EC) 45/2001 which implemented Directive 95/46/EC and Directive 97/66/EC, the predecessor of Directive 2002/58/EC, for EU institutions and bodies.[65] Article 286 of the EC Treaty, adopted in 1997 as part of the Treaty of Amsterdam, provided that 'Community acts' on the protection of individuals with regard to the processing of personal data and the free movement of such data should also apply at EU level, and laid down the legal basis for the establishment of an independent supervisory authority. This would not have been possible without such a specific legal basis. Regulation 45/2001 lays down a complete set of rules in one instrument and establishes the European

[62] Case C-553/07, *Rijkeboer*, [2009] ECR I-03889, at 56-70.
[63] 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), OJ L 201, 31.7.2002, p. 37 (e-Privacy Directive). See notably Article 1 on the scope and aim of the Directive.
[64] See e.g. *Lindqvist* and *Google Spain*.
[65] 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, OJ L 8, 12.1.2001, p. 1.

Data Protection Supervisor with a number of tasks and powers based on those set out in Directive 95/46/EC.[66]

The third category is a little different. So far we have basically dealt with the internal market legal basis in what used to be the 'first pillar' of the EU. This obviously did not apply to the other pillars such as the common foreign and security policy ('second pillar') and the police and judicial cooperation in criminal matters ('third pillar'), both introduced in the Treaty of Maastricht in 1992. The Treaty of Amsterdam transferred some of the areas covered by the third pillar - such as immigration, asylum and border control - to the first pillar, thus bringing those areas within the scope of Directive 95/46/EC. A few regulations with considerable data protection relevance have been adopted against this background.[67]

The third pillar provisions of the EU Treaty nevertheless contained some specific legal bases for legislation on data protection. The approach was here that common action in the field of police cooperation or judicial cooperation in criminal matters should be subject to appropriate safeguards on the protection of personal data, and that common standards on data protection could also contribute to the efficiency and legitimacy of the cooperation.[68] This led to a number of decisions on specific subjects, including Eurojust and Europol[69], and in 2008 also to Council Framework Decision 2008/977/JHA with general rules on the protection of personal data processed in the context of police and judicial cooperation in criminal matters.[70] The content of these rules was inspired by Directive 95/46/EC and the Council of Europe Convention 108, but the level of protection was much lower in terms of scope and substance.[71] As to the scope, the Decision only applies when personal data are transmitted or made available to other Member States, and therefore does not extend to 'domestic' processing, unlike Directive 95/46/EC.[72]

---

[66] See Articles 41-48 on the EDPS. These provisions have served as a benchmark in the CJEU judgments on the independence of supervisory authorities (see footnotes 51-52, and notably *Commission v Germany*, at 26-28).

[67] E.g. Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, p. 1 (see notably Recitals 15-17), and Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, p. 60 (see notably Recitals 17-20, also mentioning coordinated supervision by national DPAs and EDPS).

[68] See Articles 30-31 TEU before entry into force of Lisbon Treaty.

[69] Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 138, 4.6.2009, p. 14, and Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ L 121, 15.5.2009, p. 37.

[70] 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, OJ L 350, 30.12.2008, p. 60.

[71] See the Commission's own assessment when explaining the need to replace the Decision (see footnotes 124, 128 and 133).

[72] See notably Recital 7 and Article 1.

B. Charter of Fundamental Rights

Fundamental rights as guaranteed by the ECHR or resulting from the constitutional traditions common to the Member States have long been recognized and applied by the European Court of Justice as general principles of EU law. In June 1999, the European Council nevertheless decided that it was time to draw up a Charter of fundamental rights of the EU, in order 'to make their overriding importance and relevance more visible to the Union's citizens'.[73] This resulted, in December 2000 at the European summit in Nice, in the proclamation of the Charter of Fundamental rights of the European Union, initially only as a political document.[74]

One of the novel elements of the Charter was that *in addition* to the right to respect for private life, it also contained an explicit recognition of the right to the protection of personal data in a separate provision. Article 7 concerning '*Respect for private and family life*' states that 'everyone has the right to respect for his or her private and family life, home and communications'. Article 8 on '*Protection of personal data*' provides, in its first paragraph, that 'everyone has the right to the protection of personal data concerning him or her'. In the second paragraph, it provides that 'such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law', and that 'everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'. In the third paragraph, it states that 'compliance with these rules shall be subject to control by an independent authority'.

According to the explanatory notes, the rights guaranteed in Article 7 of the Charter correspond to those guaranteed by Article 8 ECHR.[75] Both are typical examples of classical fundamental rights, where *interference* is subject to strict conditions. The only difference between them is that Article 52 of the Charter contains a more general exception clause.

---

[73] Cologne European Council, 3-4 June 1999, Conclusions of the Presidency, at points 44-45 and Annex IV. A Convention made up of 15 representatives of the Heads of State and Government, 30 representatives of the national parliaments, 16 representatives of the European Parliament and 1 representative of the Commission, chaired by Mr Roman Herzog, former President of the Federal Republic of Germany and of the German Constitutional Court, was established to draw up the Charter.

[74] Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000, p. 1. The Charter was solemnly proclaimed by the European Parliament, the Council and the Commission, which committed to respecting it in their activities. The Preamble highlights that the Charter reflects '*common values*' and 'reaffirms ... the rights as they result, in particular, from the constitutional traditions and international obligations *common to the Member States*, the Treaty on European Union, the Community Treaties, the European Convention for the Protection of Human Rights and Fundamental Freedoms, ... and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights.' (emphasis added)

[75] Explanations relating to the Charter of Fundamental Rights of the European Union, document CONVENT 49 of 11.10.2000, explanation on Article 7. The Bureau of the Convention prepared these explanations for each article of the Charter. They were intended to clarify the provisions of the Charter, indicating the sources and scope of each of the rights set out therein. They had initially no legal value and were only published for information. However, the third subparagraph of Article 6(1) TEU has changed their status. A slightly revised version was published in OJ C 303, 14.12.2007, p. 17 and referred to in the preamble of the final version of the Charter in OJ C 303, 14.12.2007, p. 1. See also later publications of the Charter in OJ C 83, 30.3.2010, p. 389 and OJ C 326, 26.10.2012, p, 391.

The explanation on Article 8 mentions that it is based on Article 286 EC Treaty and Directive 95/46/EC as well as on Article 8 ECHR and on the Council of Europe Convention 108. It also observes that 'the right to protection of personal data is to be exercised under the conditions laid down in the above Directive, and may be limited under the conditions set out by Article 52 of the Charter'.[76] This leads to questions about the nature of the new right and its different elements as set out in Article 8, and about the distinction between conditions for the 'exercise' of the right laid down in Directive 95/46/EC and conditions for the 'limitation' of the right set out in Article 52.

As we have seen, the right to the protection of personal data was conceived by the Council of Europe and developed in Convention 108 in order to provide a *proactive* protection of the rights and freedoms of individuals with regard to all processing of personal data, regardless of whether such processing was an interference with the right to respect for private life or not. This was intended as a system of 'checks and balances' to provide a *structural* protection to individuals in a wide range of situations, both in the public and in the private sector.

Directive 95/46/EC has used Convention 108 as a starting point for the harmonisation of data protection laws in the EU, and specified it in different ways.[77] This involved the substantive principles of data protection, the obligations of controllers, the rights of data subjects, and the need for independent supervision as main structural elements of data protection. However, the nature of data protection as a system of 'checks and balances' to provide protection whenever personal data are processed was not changed. In other words: Articles 7 and 8 do not have the same character and must be clearly distinguished.[78]

The Convention which prepared the Charter before it was adopted at the summit in Nice had also considered including a right to informational self-determination in Article 8, but this was rejected. Instead, it decided to include a right to the protection of personal data, to preserve the main elements of Directive 95/46/EC, as the explanation briefly highlights.[79] Thus the

[76] See footnote 75, explanation on Article 8. The revised version has inserted a reference to Article 16 TFEU and Regulation 45/2001 and now states that '[the] above-mentioned Directive and Regulation contain conditions and limitations for the exercise of the right to the protection of personal data.' The reference to Article 52 has now disappeared.
[77] See *supra* Section 3, Parts A and B.
[78] This position goes further than the analysis by J. Kokott and Ch. Sobotta, 'The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', in H. Hijmans and H. Kranenborg (ed.), *Data Protection Anno 2014: How to Restore Trust?* (2014) at 83-95 and an earlier version in *International Data Privacy Law*, 2013, Vol. 3, No 4, at 222-228.
[79] See footnote 76. It should be noted that the Article 29 Working Party was indirectly involved in the work of the Convention. Its vice-chairman (1998-2000) and chairman (2000-2004), professor Stefano Rodota, was also a member of the Convention. At an early stage, the Working Party adopted a recommendation to include a fundamental right to data protection in the Charter (see Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights, adopted on 7 September 1999 (WP 26), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp26_en.pdf). Finally, the chairman of the Convention, as former president of the

essential elements set out in Article 8(2) and 8(3) correspond with the key principles of Directive 95/46/EC, such as fair and lawful processing, purpose limitation, rights of access and rectification, and independent supervision. This suggests that a 'limitation' of the right to data protection only arises where these main elements of data protection are not respected. Directive 95/46/EC and Convention 108 already provide for certain exceptions from the basic principles, where these are necessary for legitimate reasons. The distinction between conditions for the 'exercise' and conditions for the 'limitation' of the right to data protection is therefore already incorporated in the current legal framework.

Moreover, it cannot be excluded that the Court of Justice might find other main elements of data protection which have not been expressed in Article 8(2) and 8(3), but are available in Directive 95/46/EC and may be seen as implied in Article 8(1) of the Charter. Such elements might also help to reinforce the elements which have already been made explicit and further develop the impact of the general right expressed in Article 8(1).[80]

In any case, this means that the *scope* of Article 8 - involving all processing of personal data - should not be confused with the question whether the fundamental right of Article 8 has been *interfered* with. An interference with Article 8 does not arise from the mere fact that personal data are processed. Such interference can only be established if one or more of the main elements of the right to data protection - such as the need for a 'legitimate basis laid down by law' or 'independent supervision' - have not been respected. Any limitation of the right should be addressed under Article 52 and not read in the requirement of Article 8(2) for a legitimate basis in law. This requirement is not an exception clause, but an element of the right to data protection itself. It may be that the drafters of the Charter were not fully aware of this, but the explanatory note is fully in line with the approach suggested here.[81]

C. Impact of Lisbon Treaty

The entry into force of the Lisbon Treaty in December 2009 had an enormous impact on the development of EU data protection law.

In the first place, the Charter was given the same legal value as the Treaties in Article 6(1) of the Treaty on European Union (TEU). It thus became a binding instrument, not only for the EU institutions and bodies, but also for the Member States acting within the scope of EU

German Constitutional Court, must have highlighted the right to 'informational self-determination' (see footnote 73).

[80] An example could be the principle of 'purpose limitation', which has been expressed only partly in Article 8(2) ('processed ... for specified purposes'), but plays a crucial role in practice. See more in detail Article 29 Working Party, Opinion 3/2013 on purpose limitation, adopted on 2 April 2013 (WP203), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last accessed 31 May 2014)

[81] See also the slight differences between the original and the revised versions of the explanations on Article 8 as highlighted in footnote 76.

law.[82] The right to the protection of personal data was moreover specifically mentioned in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) among the general principles of the EU.[83] This meant that some of the main elements of Directive 95/46/EC have now reached the level of EU primary law. This is also relevant for the current reform, as we will see at a later stage.[84]

In the second place, Article 16(2) TFEU now provides a general legal basis for the adoption of rules by the European Parliament and the Council, acting in the normal legislative procedure, 'relating to the protection of individuals with regard to the protection of personal data' by EU institutions and bodies and by the Member States acting within the scope of EU law, and 'the free movement of such data'. Finally, like Article 8(3) of the Charter, Article 16(2) also underlines that compliance with these rules should be subject to the control of independent authorities.[85]

The terminology used in the main text recalls Directive 95/46/EC, but the scope of this new legal basis, which has been formulated as an obligation, goes in reality far beyond the internal market and covers in principle all EU policy areas.[86] The term 'rules' allows the use of directives and directly applicable regulations, and the choice between the two now largely seems a political one. At a later stage, we will consider how much discretion the legislator enjoys under Article 16(2) TFEU in the light of the Charter.[87]

In the third place and in a much wider sense, the Lisbon Treaty also reshaped the institutional structure of the EU.[88] It did largely away with the old pillar structure and introduced the proven Community method for decision making also in areas, where unanimity had been the practice in Counsel, and the Parliament only had an advisory role. Instead, the Commission now came in its usual role as initiator for new legislation, to be adopted by Parliament and Council in co-decision, each of them acting with majorities depending upon the subject. After

[82] See Article 6(1)-(2) TEU and Article 51 of the Charter. See also *infra* Section 4, Part D, on relevant case law.
[83] Article 16(1) TFEU: 'Everyone has the right to the protection of personal data concerning *them*' (emphasis added to highlight a small linguistic difference).
[84] See *infra* notably in Section 7, Part A.
[85] The small linguistic difference with Article 8(3) of the Charter ('authority' or 'authorities') does not appear to have any consequences.
[86] Article 39 TEU provides a specific legal basis for the Common Foreign and Security Policy, according to which 'the Council shall adopt' any relevant rules on data protection without the involvement of the Parliament. Declaration 20 adds that whenever 'rules ... to be adopted on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter'. Moreover, Declaration 21 acknowledges that 'specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation ... may prove necessary because of the specific nature of these fields.'
[87] See *infra* Section 7, Part A.
[88] This paragraph is obviously a very brief summary of the main changes in the Treaties, relevant in this context.

a period of transition, the Court of Justice would also be able to fully exercise its judicial role and the Commission its role as guardian of the Treaties in the enforcement of EU laws.[89]

This also meant that legislation on data protection in the former third pillar which had been adopted by the Council acting alone - sometimes even just before the Lisbon Treaty entered into force[90] - would have to be replaced by rules adopted by Parliament and Council in co-decision so as to be in line with Article 16(2) TFEU. This has added to the dynamic context of the current review of the EU legal framework for data protection.

D. Relevant Case Law

In the meantime, the Charter is playing an increasingly important role in the case law of the Court of Justice. As to the scope of the Charter, the Court has ruled that it applies whenever Member States are acting within the scope of EU law.[91] National law will in those cases have to respect the level of protection provided for in the Charter and the primacy, unity and effectiveness of the EU law at stake.[92] This may even imply that a constitutional provision at national level will no longer be applicable.[93] However, it also means that the Charter will fully apply within the scope of EU data protection law, both for the legislator itself and at a later stage.

As to the requirement of 'complete independence' for a supervisory authority, the first ruling on the subject was handed down a few months after the entry into force of the Lisbon Treaty, but the Court did not make a reference to the Charter.[94] However, in three subsequent cases it underlined that the requirement of independent supervision is an 'essential component' of the protection of personal data, and derives from Article 8(3) Charter and Article 16(2) TFEU.[95] It must therefore be assumed that the Court has now also expressed a view on the meaning of those provisions of primary law.

In recent years, the Court has twice ruled that provisions of EU law were invalid as a result of unjustified interference with Articles 7 and 8 of the Charter. In November 2010, this was the case with provisions on the publication of information on beneficiaries of agricultural aid on a website.[96] In April 2014, it happened to the mandatory retention of communication data for law enforcement purposes in the context of Directive 2006/24/EC.[97] In a third case, however,

[89] The transitional period will end on 1 December 2014 (see Article 10 of Protocol 36 on transitional provisions, attached to the Lisbon Treaty).
[90] See e.g. the Council Decisions mentioned in footnotes 69 and 70.
[91] Case C-617/10, *Åkerberg Fransson*, 26 February 2013, at 17-21, not yet published
[92] Case C-399/11, *Melloni*, 26 February 2013, at 59-60, not yet published., and *Åkerberg Fransson*, at 29.
[93] *Melloni*, at 64
[94] *Commission v Germany*, see footnote 51
[95] *Commission v Austria*, at 36-37 and *Commission v Hungary*, at 47-48 (see for both footnote 52), as well as *Digital Rights Ireland* (see footnote 97), at 68.
[96] Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert*, [2010] I-11063
[97] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger*, 8 April 2014, not yet published.

in October 2013, the Court ruled that an obligation to provide for fingerprints to be stored in a passport was valid.[98] All these cases involved requests for preliminary rulings from national courts on the validity of EU laws.

Although the outcome of these three cases is sound and convincing, they also illustrate a clear tendency of the Court towards a 'combined reading' of Articles 7 and 8 of the Charter. This approach does however not take account of the essential difference in character between these two provisions and thus may prevent Article 8 from reaching its full potential.[99]

The first of the three cases was initiated by German farmers who objected to the publication of their contact details and annual amounts in agricultural aid received. The referring court considered that the obligation to publish those data on a website constituted an unjustified interference with the fundamental right to the protection of personal data, which it felt was essentially covered by Article 8 ECHR.[100]

The Court of Justice noted that since the Lisbon Treaty had entered into force, the validity of the obligation had to be assessed in the light of the Charter.[101] It also observed that the right to the protection of personal data, as set out in Article 8 Charter was closely connected to the right to respect for private life expressed in Article 7 Charter, but was not an absolute right. This follows from Article 8(2) which authorises the processing of personal data if certain conditions are satisfied, and from Article 52(1) of the Charter which accepts that limitations may be imposed on the exercise of rights as set out in Articles 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights, and subject to the principle of proportionality are necessary and meet objectives of general interest or the need to protect the rights and freedoms of others. It also observed that these limitations correspond to those tolerated in relation to Article 8 ECHR.[102]

The Court then set out to ascertain whether the relevant provisions of EU law interfere with the rights guaranteed by Articles 7 and 8 of the Charter, and if so, whether such interference is justified having regard to Article 52 of the Charter. As to the first question, relying on the case law of the European Court of Human Rights on Article 8 ECHR and its own position in *Österreichischer Rundfunk*, it concluded that the publication of precise income data on a website constitutes an interference with the right to respect for private life within the meaning of Article 7 Charter.[103] It also found that the publication was processing of personal data

[98] Case C-291/12, *Michael Schwarz v Stadt Bochum*, 17 October 2013, not yet published. Unlike *Schecke* and *Digital Rights Ireland*, this judgment was not delivered by the Grand Chamber.
[99] For a critical analysis, see also H. Kranenborg, Commentary on Article 8, in S. Peers *et al*. (eds.), *The EU Charter of Fundamental Rights: a Commentary* (2014, 223) at 229-231 and 260-262.
[100] *Schecke*, at 30-31 and 44
[101] *Schecke*, at 45-46
[102] *Schecke*, at 47-52
[103] *Schecke*, at 56-59

within the scope of Article 8.2 of the Charter, and that the farmers had not consented to the publication, so that there had also been an interference with the right to the protection of personal data in Article 8 Charter.[104] As to the second question the Court essentially found that the interference was not justified as there was no real evidence that the legislator had considered any less intrusive alternatives.[105]

This last conclusion sends a powerful message about the need for an empirical basis for any intrusive measures. However, the conclusion that the publication interfered with both Article 7 and Article 8 Charter does not seem fully convincing. The absence of consent was in any case more relevant for Article 7 than for Article 8, in spite of the fact that Article 8(2) specifically mentions consent as *one example* of a legitimate basis for processing of personal data. The point is that valid consent would very likely have prevented a finding that Article 7 had been interfered with, whereas the Court did not pay any attention to the second option set out in Article 8(2), namely 'some other legitimate basis laid down by law'. It would then have found that the answer to the question whether this option applied could only depend on its analysis of Article 7 and not at the same time on Article 8. Indeed, the fact that the publication was processing of personal data within the scope of Article 8(2) did not make it an interference with Article 8 in the absence of only one of a number of alternative options for legitimacy. However, it is clear that the very fact that the publication was an unjustified interference with Article 7, also demonstrated that it did not comply with the requirements of Article 8(2), and that is what the Court perhaps should have said.

The approach of the Court is even more explicit and sweeping in its second ruling mentioned above concerning the storage of fingerprints in a passport. In this case a German national refused to have his fingerprints taken and disputed the validity of the relevant provisions as an infringement of the rights laid down in Articles 7 and 8 of the Charter.[106]

In response, the Court started from a 'joint reading' of those articles, while saying that, as a general rule, any processing of personal data by a third party may constitute a threat to those rights.[107] Apart from the term 'threat' which is much wider than 'infringement', this starting point seems to confuse the wide scope of Article 8 - in principle covering all processing of personal data - with the substantive question when Article 7 or Article 8 has been interfered with. Moreover, from the fact that taking a person's fingerprints and storing those fingerprints in a passport can be viewed as processing of personal data, the Court subsequently concludes that the taking and storing of fingerprints on the basis of the relevant provisions constitutes a threat to the rights to respect for private life and the protection of personal data.[108]

[104] *Schecke*, at 60-64
[105] *Schecke*, at 81-86
[106] *Schwarz*, at 12
[107] *Schwarz*, at 23-25
[108] *Schwarz*, at 26-30

In its analysis of the justification of this 'twofold threat', the Court first observes that persons are not free to object against the processing of their fingerprints and that persons applying for passports can therefore not be deemed to have consented to that processing.[109] The Court then considers whether the processing of fingerprints can be justified 'on the basis of some other legitimate basis laid down by law'. After substantial analysis in the light of Article 52(1) of the Charter, the Court concludes that this is indeed the case for the relevant provisions as to both Article 7 and Article 8 of the Charter.[110]

It is striking to see how this analysis was entirely focussed on the processing of personal data and the conditions of Article 8 and Article 52(1) of the Charter. A more convincing alternative approach would have been that the Court - fully in line with the case law of the Court of Human Rights[111] - would have found that the taking and storing of fingerprints was an interference with the right to respect for private life in Article 7, but was justified according to the criteria of Article 52(1). Instead the Court apparently saw an interference with Article 8 before it had verified whether there was 'another legitimate basis laid down by law'. Paradoxically, the conclusion that the relevant provisions were indeed valid, only confirms that the finding of an infringement of Article 8 had been premature.

In the third ruling mentioned above concerning the mandatory retention of communication data for law enforcement purposes, the Court was asked to examine the validity of the Data Retention Directive[112] in the light of Articles 7 and 8 of the Charter. In this case, the Court focussed much more on Article 7 on the right to respect for private life and found that the interference with this right had been 'wide-ranging' and 'particularly serious', and could not be justified.[113] However, it also mentioned Article 8 on the right to the protection of personal data in that context.

In its preliminary remarks the Court first observed that 'such retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article'.[114] The Court then observed that 'whereas the references for a preliminary ruling in the present case raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers

[109] *Schwarz*, at 32
[110] *Schwarz*, at 33-34 and 63
[111] See e.g. *S and Marper v United Kingdom*, Applications 30562/04 and 30566/04, ECHR 2008-V, at 78-86.
[112] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54.
[113] *Digital Rights Ireland*, at 37 and 70
[114] *Digital Rights Ireland*, at 29

and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter'.[115] Both statements correctly reflect a particular view on the role of Article 8: it is seen as a source of *requirements* for the processing of personal data within its scope. However, a few paragraphs later the Court suddenly observes: 'Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.[116]

This last observation is not compatible with the two previous statements and with the difference in character between Articles 7 and 8. Once again the Court concludes that there has been an interference with Article 8 before verifying whether 'the requirements arising from that article' have been fulfilled. In effect, Article 8 permits the processing of personal data so long as its requirements are satisfied. In this case, the answer would have been that the 'legitimate basis laid down by law' was missing, but that conclusion could only be drawn after an analysis of the possible justification of the interference. In any event, the Court's ruling makes abundantly clear that such a justification was lacking.

The three cases therefore illustrate that the Court still seems to be struggling with the proper role of Article 8 Charter. In the cases on the independence of supervisory authorities, this role was obvious: an 'essential component' of the protection of personal data in Article 8(3) was missing.[117] Similarly there could be an interference with Article 8 if one or more of the other essential elements in that article - such as fair processing, purpose limitation, rights of access and rectification - were not complied with. Whether such a limitation is justified or not will subsequently depend on an assessment in the light of Article 52.

5. The Review of Directive 95/46/EC

A. Origin of the Review

Article 33 of Directive 95/46/EC requires the Commission to report at regular intervals on the implementation of the Directive and to submit suitable proposals for amendments if needed.

The first report was published in May 2003, after an extensive open review process.[118] This report highlighted a number of problems, among which were considerable divergences

[115] *Digital Rights Ireland*, at 30
[116] *Digital Rights Ireland*, at 36
[117] See references in footnotes 94 and 95. However, in these cases, 'interference' with Article 8(3) Charter was not explicitly mentioned.
[118] First report on the implementation of the Data Protection Directive (95/46/EC), 15.5.2003, COM (2003) 265 final. See also the very informative technical annex: 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States'. Both documents are available at: http://ec.europa.eu/justice/data-protection/document/transposition/index_en.htm (last accessed 31 May 2014).

between Member States, either due to incorrect implementation or different policy choices within the margins of the Directive. However, as practical experience with the Directive was limited, the Commission felt it was too early for amendments. It preferred a work programme for better implementation, with different tasks for the Commission, the Member States, supervisory authorities and other interested parties. The report also called on the Article 29 Working Party to encourage better enforcement and joint investigations in relevant sectors.

In a second report, on the follow up of the work programme[119] in March 2007, the Commission mentioned that some of the problems highlighted still existed, but did not pose a real problem for the internal market. As the legal solutions provided by the Directive were still appropriate and could also be applied to new technologies, the Commission again considered that it was too early for amendments and encouraged all actors to continue their efforts in the context of the work programme. In July 2007, the European Data Protection Supervisor agreed that it was still not the right time to amend the Directive, but also took the position that change was unavoidable and should be prepared well.[120]

Shortly afterwards, and with some reluctance, the Commission started preparations. In May 2009, it launched a public consultation about the need for change of the legal framework for data protection.[121] This resulted in a very large number of reactions from a wide range of stakeholders, including a substantial contribution from the Article 29 Working Party on 'the Future of Privacy'.[122] This coincided with the entering into force of the Lisbon Treaty in December 2009, which introduced a new horizontal legal basis for data protection, and with the appointment of a new Commission with a stronger human rights agenda.[123]

In November 2010, the Commission published the outline of a 'comprehensive approach on data protection in the EU', which it intended to build on this new legal basis.[124] Its approach was to 'strengthen the rights of individuals', 'enhance the internal market dimension', 'ensure

[119] Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, 7.3.2007, COM (2007) 87 final, availabe at: http://ec.europa.eu/justice/data-protection/law/follow-up-work-programme/index_en.htm (last accessed 31 May 2014).

[120] Opinion of the EDPS of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, OJ C 255, 27.10.2007, p. 1

[121] See information available at: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm (last accessed 31 May 2014).

[122] Article 29 Working Party & Working Party on Police and Justice, 'The Future of Privacy', Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009 (WP 168), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

[123] Ms Viviane Reding, Vice-President of the Commission, responsible for Justice, Fundamental Rights and Citizenship, made the data protection reform one of her top priorities.

[124] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: 'A comprehensive approach on personal data protection in the European Union', COM (2010) 609 final. See also V. Reding, 'The upcoming data protection reform for the European Union', *International Data Privacy Law*, 2011, Vol. 1, No. 1, at 3-5.

better enforcement of data protection rules', and also cover 'the global dimension of data protection'. Proposals for a new framework were expected to be submitted in 2011.[125] As a second step, the Commission would assess the need to adapt other legal instruments to this new general framework, in which it would also involve Regulation 45/2001 applying to EU institutions and bodies.[126] In January 2011, the European Data Protection Supervisor expressed support for the main lines of the Communication, but asked for a more ambitious approach on a number of points.[127]

B. Main Lines of the Review

In January 2012, only slightly later than announced, the Commission presented a package of proposals in order to update and modernise the present EU legal framework.[128] This package has since then been the subject of intense discussions, both inside and outside the European Parliament and the Council, and the review is now approaching the final stage of political decision making: negotiations between the Parliament and the Council about the first tangible outcomes.[129]

Before going further into the substance, it is helpful to sum up briefly why the current review is taking place. This is basically for three reasons. The first reason is that there is a clear need to update the present framework, more specifically Directive 95/46/EC as its central element. The term 'updating' means in this case, most of all, ensuring its continued *effectiveness* in practice. When the Directive was adopted, the Internet barely existed, whereas we now live in a world where data processing has become ubiquitous, so that we also need stronger safeguards that deliver acceptable results in practice. The challenges of new technologies and globalisation require some imaginative innovation to ensure a more effective protection.

The second reason is that the present framework has led to some degree of harmonisation, but also to increasing *diversity* and *complexity*, if only for the reason that a directive - according to its legal nature - must be transposed into national law and we now are confronted with 28

[125] COM (2010) 609 final, at 18

[126] Ibid., at 18-19

[127] Opinion of the EDPS of 14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - 'A comprehensive approach on personal data protection in the European Union, OJ C 181/01, 22.06.2011, p.1

[128] See Communication from the Commission to the European Parliament, the Council, the 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) 9 final. See also: V. Reding, 'The European data protection framework for the twenty-first century', *International Data Privacy Law*, 2012, Vol. 2, No. 3, at 119-129, and C. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', Bloomberg BNA *Privacy and Security Law Report*, 11 PVLR 215, 02/06/2012, at 1-15.

[129] In March 2014, the European Parliament adopted its positions on the proposed Regulation and the proposed Directive in first reading with overwhelming majorities. Discussions in Council have made less progress. The Council is following a 'partial general approach' on various subjects and is expected to reach a general position by the end of 2014. In June 2014, it adopted a 'partial general approach' on the territorial scope and Chapter V of the Regulation concerning transfer of personal data to third countries or international organisations.

sometimes very different versions of the same basic principles. That is obviously too diverse and results not only in unnecessary costs, but also in a loss of effectiveness. The first report on the implementation of the Directive documented a series of differences between national laws in scope and definitions as well as in practices for application and enforcement.[130] The efforts to reduce those differences have clearly not been sufficiently productive. At the same time, the need for more harmonised rules has increased as result of technological change and globalisation. In other words, there is a need to scale up harmonisation, and make the legal system not only stronger and more effective, but also more *consistent*. This should lead to a reduction of the current *unhelpful* diversity and complexity.

The third reason has to do with the new institutional framework of the EU. As we have seen, the Lisbon Treaty has placed a considerable emphasis on the protection of fundamental rights, and especially on the right to data protection. A separate right to the protection of personal data was laid down in Article 8 of the Charter, and a new horizontal legal basis in Article 16 TFEU for the adoption of rules on data protection, providing for comprehensive protection in *all* policy areas, regardless of whether this relates to the internal market, law enforcement, or almost any other part of the public sector.[131]

The current review is therefore about stronger, more effective, more consistent, and more *comprehensive* protection of personal data. The term 'comprehensive' was also used by the Commission in its strategy for the reform, albeit in a much more general way: it mentioned a comprehensive 'approach' to be delivered in different stages.[132]

The package of proposals presented by the Commission in January 2012 consists of two main elements: a proposal for a General Data Protection Regulation to replace the current Directive 95/46/EC for the private sector and most of the public sector in the Member States, and a proposal for a Directive to replace the current Council Framework Decision 2008/977/JHA for the area of criminal law enforcement.[133]

The proposal for a Regulation has been welcomed as a 'huge step forward'[134] towards a more effective and consistent protection of personal data across the EU, but it also required some

[130] See especially the annex mentioned in footnote 118.
[131] See *supra* Section 4, Part C
[132] See footnote 124
[133] 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, and
- Proposal for a Directive of the European Parliament and of the Council 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.
[134] Press release of the EDPS, 25 January 2012, available at:

clarification and improvement on a number of important details. These points have been developed in the detailed Opinion of the EDPS of March 2012.[135] The circumstance that the proposed Regulation would be directly binding in all Member States made it all the more important to ensure sufficient clarity of its provisions.

However, the architecture of the package itself - a Regulation and a Directive - also signalled that there was a problem with its comprehensiveness. And indeed, this is where the main weaknesses of the package could be found. The level of protection in the proposed Directive is much lower than in the proposed Regulation.[136] This problem can be analysed on different levels: the option of a Regulation also covering the area of criminal law enforcement was apparently a bridge too far for most Member States, even with the inclusion of appropriate limitations and exceptions. The second option of a Directive with the same substance as the Regulation, but subject to the necessary limitations and exceptions, and leaving more space for domestic implementation, was quite conceivable. Yet this is not what the Commission proposed. The resulting discrepancies can be considered on their own merits, but exchange of information between public and private entities - e.g. law enforcement and banks, telephone, travelling etc - is increasing, and a lack of balance and consistency at this interface will have serious practical consequences in a wider field. It should also be noted that related areas, such as taxation, customs and border control, are already within the scope of Directive 95/46/EC and would therefore be covered by the proposed Regulation.

As to the Regulation, there are a few general points to keep in mind. The first one is that - in spite of all innovation - there is also a lot of *continuity*. All the familiar basic concepts and principles will continue to exist, subject to some clarification and smaller changes in details. An example of innovation is a much stronger emphasis[137] on 'data minimisation' - briefly put: 'no more data than strictly necessary' or 'the best protection is to process as few data as possible'. Another example is the explicit recognition of 'Privacy by Design' - briefly put: 'taking privacy into account from the start' - as a general principle.[138] There is also a welcome clarification of 'consent': *when* you need it, it must be real and robust consent.[139]

---

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-02_EC_DP_Proposal_EN.pdf (last accessed 31 May 2014)

[135] Opinion of the EDPS of 7 March 2012 on the data protection reform package, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf (last accessed 31 May 2014).
See also executive summary in OJ C 192, 30.6.2012, p. 7 and press release, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-07_DPReform_package_EN.pdf (last accessed 31 May 2014).

[136] See EDPS Opinion (footnote 135), p. 49-74

[137] Article 5 sub (c)

[138] Article 23 on 'data protection by design and by default'

[139] Article 4 sub (8) and Article 7

Where the real innovation comes, it is mainly about 'making data protection more effective in practice'. This implies, as we will see, a strong emphasis on implementation of principles, and on enforcement of rights and obligations, in order to ensure that protection is delivered where it is needed in practice. At the same time, the Regulation provides for simplification and reduction of costs. A clear example is that prior notification of processing operations to a data protection authority has been largely eliminated. This will only be required in situations of specific risks.[140] The proposed Regulation also provides for a 'one-stop-shop' for companies with establishments in different Member States. This involves the introduction of a lead DPA who is to act in close cooperation with other competent authorities involved.[141]

A directly binding Regulation will also bring greater harmonisation - in principle: one single applicable law - and greater consistency in all Member States. In itself, this will also bring an important simplification and reduction of costs for companies operating in different Member States. At the same time, this is bound to raise political issues, as it will be at the expense of national perceptions and preferences as to what is the best approach in data protection. At a more detailed level, there are also issues as to how exactly the Regulation will relate to domestic law, and how exactly the one-stop-shop feature will function. We will come back to those issues at a later stage.[142]

C. General Data Protection Regulation

It is now time to take a closer look at the main lines of the proposed General Data Protection Regulation itself. As this is a very substantial and rather complicated document, it is helpful to approach it from different angles and to look at its scope, its main points of substance, and finally at the international dimensions of the Regulation.

General Scope

The material scope of the Regulation closely resembles the scope of the current Directive: it applies to all processing of personal data wholly or partly by automated means, and to the processing by other means of personal data in or intended for a filing system, except in a few situations which in substance correspond with those mentioned in the Directive.[143] However, these exceptions also cover the processing of personal data by EU institutions and bodies. Although this was intended as a technical exception to be followed by a separate proposal at a later stage, it has rightly raised the question why the EU level itself should be left for a second phase.[144]

[140] Article 33 and 34
[141] Article 51 (2)
[142] See *infra* Section 6, Parts A and C
[143] Article 2
[144] Article 2 (2)(b). Both Parliament and Council have threatened to delete the exception, unless the Commission comes up with a separate proposal which is fully consistent.

In any case, it should be underlined that the Regulation has a general scope: it will apply both in the private and the public sector.[145] This is completely consistent with the situation under the present Directive. The possibility of a systematic distinction in this Directive between the public sector and the private sector was explicitly considered and rejected.[146] This approach has proved to be quite feasible in practice, as some of its provisions - especially those on lawful processing, referring to 'public tasks' - are obviously more relevant for public bodies, and other provisions - referring to 'contracts' or 'legitimate interests' - are more relevant for private actors.[147]

The Court of Justice has confirmed that the present Directive also applies in the public sector of a Member State.[148] However, it also emphasized that national law can only serve as a legitimate ground for processing if it fully complies with fundamental rights.[149] This position is reinforced by the fact that Article 8 Charter now also contains an explicit recognition of the right to the protection of personal data, and that Article 16 TFEU provides for an explicit horizontal legal basis for the adoption of rules on the protection of personal data, both at EU level and in the Member States, when they are acting within the scope of EU law, regardless of whether it relates to the private or the public sector.

At the same time, it is necessary to make a closer analysis of the relationship between EU law and national law on the basis of the proposed Regulation. The impression that the Regulation will simply replace all relevant national law is not correct. This depends also on the way in which the Regulation itself deals with this relationship. In this respect, there are different ways in which national and EU law will co-exist and interact. For example, the Regulation will build on national laws that fully comply with fundamental rights.[150]

In addition, it should also be considered very carefully whether - and if so where and how - the Regulation should allow more space for specification of its provisions in national law. However it would not be useful to consider a splitting up of the Regulation into two different instruments - one for the public sector and another one for the private or commercial sector. To the contrary, such a change would have a disastrous impact, both on the effectiveness and on the consistency of the new framework, particularly for services at or across the dividing line between the two areas. The distinction would probably also work out differently for different Member States, and thus easily lead to new discrepancies and undermine the internal market in cross-border situations.

---

[145] Article 2 and all other general provisions do not distinguish between public and private sector.
[146] The first Commission proposal on the Directive (see footnote 31) was based on a systematic distinction, but was later replaced by a revised proposal with a more general scope.
[147] See Article 7 sub (b), (e) and (f) of Directive 95/46/EC
[148] *Österreichischer Rundfunk*, at 47 (footnote 53). See also: Case C-524/06, *Huber*, [2008] ECR I-09705 and *Rijkeboer* (footnote 62)
[149] *Österreichischer Rundfunk*, at 68-72
[150] See *infra* Section 6, Part A.

As to the substance of the Regulation, it strengthens the roles of the key players: the individual (data subject), the responsible organisation (controller), and the supervisory authorities. This leads to three different perspectives which together amount to stronger data protection.

User Control

The first perspective may also be seen as enhancing the control of data subjects over the processing of their personal information. There is no doubt that ensuring an effective control for data subjects is an important *objective* of data protection law, even if this is not the same as endorsing the formal right to informational self-determination. Article 8(2) of the Charter also underlines the importance of this control by referring to the rights of access and rectification.

It should be noted that the current rights of the data subject have all been confirmed in the Regulation, and at the same time strengthened or even extended.[151] The requirement for free, specific, informed, and unambiguous consent has been clarified and slightly reinforced by the condition that it should also be 'explicit'. This is a welcome reaction to a widespread practice on the Internet building on consent under very ambiguous circumstances. At the same time, the Regulation is flexible enough to be satisfied with a clear affirmative action.[152]

There is also a stronger right to object: it does not require the data subject to show a compelling legitimate ground to object and instead requires the controller to justify the compelling need for the processing.[153] In addition there are stronger means to ensure that the rights of the data subject are respected in practice.[154] There is more emphasis on transparency,[155] and there is a provision introducing a collective action, not a class action in US style, but still one which allows organisations to act on behalf of their members or constituencies.[156]

There has also been much discussion about the 'right to be forgotten', but on a closer analysis, it is basically a greater emphasis on deletion of data when there is 'not a good reason to keep them',[157] together with a duty to make reasonable efforts to contact third parties so as to undo the effects of publication of data on the Internet.[158] The right to 'data portability' is basically a

[151] See notably Articles 11-19, now also providing uniform rules across the EU.
[152] Article 4 sub (8)
[153] Article 19
[154] Article 12 provides, for instance, for an adequate 'infrastructure': it requires the controller to 'pro-actively' establish procedures for the exercise of the data subject's rights.
[155] See Article 11 on transparent and easily accessible policies, and transparent information and communication.
[156] Articles 73-76.
[157] In *Google Spain* (footnote 45) at 73-74, 88, 93-94 and 98-99 the Court goes in the same direction.
[158] Article 17

specification of the present right to require communication of any personal data in an intelligible form, but now also in a particular format.[159]

Responsibility

The biggest emphasis is on real responsibility of responsible organisations. Responsibility is not a concept that only comes *at the end*, when something has gone wrong. Instead, it comes as a proactive obligation to develop adequate *data management* in practice. This appears in language such as 'taking all appropriate measures to ensure compliance', and 'verifying and demonstrating that those measures continue to be effective'.[160]

This is one of the major shifts in data protection law. It implies that the *burden of proof* is in many cases on the responsible organisation: to demonstrate that there is an adequate legal basis for processing, that consent is real consent, and that measures continue to be effective. [161] It also explains the frequent use of the term 'accountability' in relevant discussions.[162]

The Regulation also provides for a number of specific requirements, such as the need for a privacy impact assessment, the keeping of documentation, and the appointment of a data protection officer.[163] Some of those provisions, especially on documentation, were according to many observers overly detailed and have therefore given rise to much discussion, both in the Parliament and the Council. Some exceptions in the same provisions may not have been fully justified, including those for small and medium enterprise. A better balance in this part of the proposal may solve both problems. In this context, it is essential that general provisions in the current and future frameworks are inherently scalable. Inappropriate specifications may call for unnecessary exceptions. This search for the right balance is now taking place under the term 'risk-based approach'.[164]

A general provision on security breach notification is also included.[165] EU law now provides for such a notification only in the case of telecommunication providers.[166] This could be seen as a mechanism of accountability 'at the end', reinforcing 'life cycle' data management.

[159] Article 18
[160] Article 22
[161] Article 5 sub (f), Article 7(1) and Article 22(1).
[162] See Article 29 Working Party, Opinion 3/2010 on the principle of accountability, adopted on 13 July 2010 (WP 173). For more on accountability and compliance, see *infra* Section 7, Part B.
[163] Articles 22(2), 28, 33 and 35-37
[164] See *infra* Section 6, Part B
[165] Article 31
[166] Article 4 (3)-(5) of Directive 2002/58/EC (see footnote 63), as revised in 2009

Supervision and Enforcement

A third main emphasis in the Regulation is on the need for more effective supervision and enforcement. The safeguards for complete independence of supervisory authorities have been strengthened in line with the case law of the Court.[167]

The Regulation also provides for supervisory authorities with strong enforcement powers in all Member States.[168] Administrative fines of millions of euro - competition size fines – have attracted a lot of attention, but the message is: 'if this is important, it should be dealt with accordingly'. This will drive 'data protection' much higher on the agenda of corporate boardrooms, which is very welcome.

In reality, we already observe a rapidly developing practice of more vigorous enforcement, with different tools at national level: remedial sanctions, administrative fines, and also some increased liabilities. This trend will no doubt continue in the near future, if possible enhanced on the basis of the Regulation.

International cooperation among data protection authorities is also strongly encouraged and facilitated in the Regulation.[169] The introduction of a lead authority for companies with multiple establishments is welcome, but again, this lead authority will not be acting on its own, but be part of a network of close cooperation with other competent authorities.[170]

A very important additional element is the introduction of a consistency mechanism in the context of a European Data Protection Board, which is to be built on the basis of the present Article 29 Working Party. This mechanism is to ensure consistent outcomes of supervision and enforcement across all the Member States.[171]

Global Privacy

A final element is the wider international dimension of the Regulation. The scope of the new legal framework has been clarified and extended. These provisions now apply not only to all processing in the context of an establishment of the controller in the EU,[172] but also when from an establishment in a third country, goods or services are offered on the European market, or the behaviour of data subjects in the EU is monitored.[173]

This is a growing reality on the Internet nowadays. At the same time, it is a realistic approach that builds on an increasing synergy as to data protection in many relevant countries around

[167] Article 47
[168] Articles 53 and 79
[169] Articles 45 and 55-56
[170] Article 51(2) and *infra* Section 6, Part C
[171] Articles 57-61 and 64-72
[172] As recently explained in *Google Spain* (footnote 45)
[173] Article 3

the world.[174] Directive 95/46/EC has exercised a major influence on global standards and there is no reason to think that this will be different for the Regulation. The combined market power of 500 million consumers in the EU market will also help to ensure compliance.

In this respect, it is relevant to mention that the international cooperation of data protection authorities is also developing in a wider context - e.g. between the Federal Trade Commission in the US and supervisory authorities in the EU - in a global network of privacy enforcement authorities (GPEN).[175] This will make it possible to deal more effectively with global actors on the Internet. This development benefits from a growing convergence of data protection principles and practices around the world, also encouraged by the partly overlapping frameworks of the Council of Europe and the OECD. [176]

Finally, it should be mentioned that provisions on trans-border data flows in the present Directive have also been further developed and where possible simplified. There is now also a specific provision on binding corporate rules (BCR), with a number of simplifications.[177]

6. Key Issues in the Legislative Debate

A. One Single Set of Applicable Rules?

In Section 5, part B, we mentioned that the Regulation will bring greater harmonisation - in principle: one single applicable law - and greater consistency in all Member States. This is no doubt an important achievement. In the present system, the national law of a Member State usually applies to the processing of personal data carried out 'in the context of the activities of an establishment' of the controller on the territory of that Member State.[178] This leads to the result that any Member State may be confronted with different national laws on its territory, depending upon the context in which personal data are being processed. Data subjects may also be confronted with other national laws than their own. In the future, the Regulation will in principle not only determine the external scope of EU law, but also the applicable law anywhere in the EU.

But does this mean that there will be only one single set of applicable rules? The Commission has used this message repeatedly to generate support for the Regulation and it has also been an important argument for the Parliament and other stakeholders to provide that support. Yet this claim does not seem entirely justified for at least two reasons.

---

[174] See *infra* Section 6, Part D

[175] Global Privacy Enforcement Network (https://www.privacyenforcement.net), established further to OECD Recommendation of 12 June 2007 on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, available at: http://www.oecd.org/internet/ieconomy/38770483.pdf (last accessed 31 May 2014).

[176] See *infra* Section 6, Part D

[177] Articles 40-45 (see Article 43 on BCR).

[178] Article 4(1)(a). See also footnote 45.

The first reason is that the Regulation may be an important part of a comprehensive approach, but it is by no means the only part. In fact, it seems to be part of a comprehensive approach in different steps, but neither in the short or mid term, nor in the long term, is there any certainty that the Regulation would provide the only set of applicable rules for any relevant subject of data protection.[179] Instead, it will be more likely that other, perhaps more specific rules - such as the current Directive 2002/58/EC on privacy and electronic communications - would also be applicable. It would be a good result if those other rules were completely consistent with the requirements of the Regulation.

The second reason is more fundamental. As mentioned in Section 5, part C, the impression that the Regulation will replace all relevant national law is not correct. This also depends on the way in which the Regulation deals with the relationship between EU law and national law. In this respect, there are at least four different ways in which national and EU law will co-exist and interact. It may happen that the Regulation *builds* on national law, or conversely allows or mandates national law to build on and give *effect* to the Regulation. There are also examples of provisions where the Regulation allows or even requires national law to *specify* or further develop its rules in certain areas or even to *depart* from its provisions under certain conditions.[180]

Examples of the first category - *building* on national law - can be found in the provisions on the grounds for lawful processing. According to Article 6(1) of the Regulation, processing of personal data shall be lawful if and to the extent that such processing is (c) necessary for compliance with a legal obligation to which the controller is subject, or (e) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In both cases, the Regulation builds on grounds for processing which are in most cases essentially provided under national law.

In the last two categories - *specifying* or *departing* - the Regulation gives different degrees of flexibility to adopt national rules on certain subjects.[181] In some situations, this flexibility is considerable, which implies that there will be considerable scope for diversity and thus also for different applicable rules in those areas. It may well be that this simply shows the limits of harmonisation and consistency in an EU context.

In most Member States, there will be a number of national laws that may not deal with data protection explicitly, but still contain a variety of provisions on the collection, storage, exchange or publication of personal data, or on the way in which the rights of data subjects

[179] See footnote 124
[180] See EDPS Opinion of 7 March 2012 (footnote 135) at points 50-55. Articles 46-49 require Member States to establish one or more independent supervisory authorities according to these provisions. Examples of the other three categories follow immediately below.
[181] See notably Article 21 (restrictions) and Articles 80-85 (specific situations)

should be exercised or respected in a specific field. Many of these laws may come within the scope of Directive 95/46/EC and may have been part of its implementation into national law.[182] In most Member States, such laws will be consistent with the national data protection law. They will be more frequent in the public sector, but may also be relevant in other areas.

It is clear that such laws must be amended if they are not compatible with the Regulation in its final shape, to the extent in which their provisions would not provide a basis for lawful processing of personal data (as in the first category) and are not somehow provided for in the Regulation. This would require that such national laws be aligned with the provisions of the Regulation, including the general principle of free movement of personal data with the EU as now expressed in Article 1 thereof.

This brief analysis shows that there will not be one single set of applicable rules and that the establishment of the precise relationship of EU and national law will require careful study and fine tuning, both at EU and at national level. This is even more the case if the Regulation continues to apply to the private and the public sector. On the other hand, the Regulation will have accomplished an enormous and desirable step forward in ensuring greater harmonisation and consistency if these efforts are successful.

B. Administrative Burdens and Innovation

The proposed Regulation has not only been welcomed, but also heavily criticized by business organisations and it has been the subject of unprecedented lobbying campaigns. In a way, this only confirms the relevance of the subject for our digital economies, and for our increasingly ICT dependent societies as a whole. Two partially overlapping themes prevail in the critical reactions: firstly, the Regulation will create heavy administrative burdens for data controllers, particularly in small and medium enterprise, and secondly, it would stifle innovation in areas which are crucial for the development of our economies.

Both themes are remarkable because the Commission has been very keen to highlight that the proposed Regulation also provides for simplification and reduction of costs. In Section 5, part B, we have mentioned three examples: the sharp reduction of prior notification to data protection authorities, the introduction of a one-stop-shop for companies with establishments in different Member States, and a directly binding Regulation to ensure greater harmonisation and greater consistency in all Member States. It should also be noted that privacy and trust are key themes in the Commission's Digital Agenda which is an essential part of the EU 2020 strategy for a smart, sustainable and inclusive Europe.[183] Strong and effective safeguards for

[182] This may involve social security, taxation, population files, civil registry etc. See also the Court judgments mentioned in footnote 143.

[183] See http://ec.europa.eu/digital-agenda and http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_en.htm (last accessed 31 May 2014)

the protection of personal data indeed also aim to contribute to economic growth and more jobs. This discussion therefore seems to show two sides of the same coin and fits well in the search for the right balance between means and ends, and between costs and benefits. The need for proportionality is also an important, more general principle of EU law.[184]

Three comments should be made in this context. In the first place, nobody would like to see innovation stifled, but at the same time it would be foolish to close our eyes to the fact that innovation may have negative sides which public policy makers need to address. This is particularly true for the development of information technology which has now become so pervasive in our societies. The concept of data protection was conceived in order to provide legal protection of individuals against the improper or excessive use of information technology for the processing of information relating to them. The right to the protection of personal data has now become a fundamental right, and has been reinforced by a compulsory legal basis for rules designed to ensure its continued effectiveness in a modern society. However, the content of these rules must always be in keeping with the aim pursued and not go beyond this aim. At the same time, more innovation should be encouraged to take account of data protection requirements at the outset ('Privacy by Design'), which is cheaper and more effective than subsequently retrofitting technology to make it more compliant.

In the second place, it is necessary to make a clear distinction between measures to ensure compliance with existing rules and new legal requirements. It may well be that organisations which have so far underestimated or even ignored the relevance of existing rules on data protection for their particular activities[185] - either online or offline - and may therefore be in a state of non-compliance with existing law, will find themselves unpleasantly surprised by efforts to give more force and effectiveness to principles that have been around for some time. Some of the heavy lobbying against the proposed Regulation suggests that this is indeed the case for newcomers and perhaps also some successful operators on the Internet. However, that is no reason to disregard the legitimate purpose of providing better safeguards so as to ensure the continued effectiveness of a fundamental right.

In the third place, what therefore remains is the search for the right balance between the need to ensure effective protection of individuals in an often dynamic environment and the need to avoid unnecessary administrative burdens. The discussion about this subject has largely been triggered by the fact that the relevant provisions in the proposal for the Regulation did not put enough emphasis on the general principles of responsibility and accountability for controllers, but instead went too fast into specific requirements, which in turn led to a number of specific exceptions, inter alia to protect small and medium enterprise from undue administrative

[184] See Article 5 TEU and Protocol No 2 on the application of the principles of subsidiarity and proportionality annexed to the Treaties.

[185] In this respect, *Google Spain* (footnote 45) may have served as a 'wake up call' for operators to rethink their current business cases and related legal arrangements.

burdens.[186] It is true that some specifics were unavoidable to ensure a consistent application of the Regulation across the EU, but a greater emphasis on the general principles of responsibility would have provided a better framework for the analysis. One relevant question is for example what the controller's general obligation to take 'appropriate measures' entails in cases where the specific requirements do not apply.

This problem is now addressed in the context of the 'risk-based approach'. This should be carefully distinguished from the notion of 'risk' as a *threshold* condition for any protection to apply, and even more from an approach in which protection would only apply to the most risky processing operations. Indeed, it should be taken into account that risk is inherent to any data processing. A 'progressive' risk-based approach would suggest instead that more detailed obligations should apply where the risk is higher and less burdensome obligations where it is lower. This approach has two important advantages: firstly, it means that compliance efforts should be primarily directed at areas where this is most needed, having regard, for example, to the sensitivity of the data or the risk involved in a specific processing operation, rather than at a 'box-ticking' exercise to satisfy bureaucratic requirements. Secondly, it means that areas of minimal risk could be addressed in a more 'light touch' fashion. It should be emphasized however that general provisions in the current and future frameworks are inherently scalable and should therefore always be respected. The specific rights of the data subject should also be available regardless of the risk involved.

Efforts are being made to further describe the notion of 'risk', which necessarily involves a measure of judgment. In the interest of legal certainty, the Regulation should provide for sufficiently clear criteria according to which such risk assessment should be performed by controllers, including both objective factors (such as the number of individuals affected by a specific processing operation), and more subjective notions (such as the likely adverse effects on an individual's privacy).[187] On the basis of these general criteria set out in the Regulation, further guidance could be given, either by the European Data Protection Board or in delegated acts, both subject to appropriate supervision and enforcement. Such an approach would allow for more legal certainty for controllers, more effective protection for individuals, and sufficient flexibility to stand the test of time.

C. One-stop-shops for Citizens and Business

One of the new elements of the proposed Regulation is the introduction of a one-stop-shop for companies with establishments in different Member States.[188] Put simply, this means that

[186] See Articles 22-37 and *supra* Section 5, Part C

[187] A completely different element of risk is which consequences non-compliance may have for the controllers themselves in terms of sanctions, liability and loss of customers' trust.

[188] See notably Article 51(2). See also point 2 of the EDPS letter of 14 February 2014 to the Council regarding progress on the data protection reform package, available at:

when the processing of personal data takes place in more than one Member State, one single supervisory authority should be responsible for monitoring the activities of the controller or processor throughout the EU and taking the related decisions. According to the proposal, this would normally be the national Data Protection Authority (DPA) of the Member State where the 'main establishment' of the data processing entity is located, also referred to as a 'lead authority'. The role of a lead authority should *not* be seen as an *exclusive* competence, but as a structured way of cooperating with other locally competent supervisory authorities. Indeed, the lead authority will depend heavily on input and support of other DPAs at different stages of the process.

The proposed Regulation was rather ambiguous on this point. The Commission seemed to suggest that the role of a lead authority was an exclusive competence. On the other hand, the Regulation did not explicitly provide for adequate powers of the lead authority outside its own jurisdiction. At the same time, it provided for a strong link with the provisions on mutual cooperation with other supervisory authorities, which should indeed enable the lead authority to exercise its role effectively. Moreover, any decision of the lead authority would only be enforceable across the EU, if the matter had been dealt with in a consistency mechanism involving all other national supervisory authorities in the European Data Protection Board.[189] In this way, other (locally competent) supervisory authorities would be able to participate in and influence the outcome of the cooperation and the final decision of the lead authority in all relevant cases.

The one-stop-shop principle is an important element of the harmonisation of the EU legal framework for data protection. It has been proposed by the Commission in order to increase the consistent application, provide legal certainty and reduce undue administrative burden for controllers and processors that are active in more than one Member State. It also reduces the fragmentation of the data protection landscape. It is important for business to be able to deal with (ideally) one interlocutor instead of (potentially) 28 national regulators.

Although the Council endorsed the principle in October 2013, it subsequently also considered a number of objections against the one-stop-shop principle raised by its own Legal Service.[190] These questioned its compatibility with the Charter of Fundamental Rights, in particular with Article 47, which provides for the right to an effective remedy before a tribunal and the right to a fair trial, in substance corresponding to Article 13 and 6(1) of the ECHR. The key concern seemed to be the issue of 'proximity' between the lead DPA taking a decision in a

---

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-02-14_letter_Council_reform_package_EN.pdf (last accessed 31 May 2014)

[189] Article 63

[190] See Note of the Presidency of 26 May 2014 to the Council on the one-stop-shop mechanism, available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010139%202014%20INIT (last accessed 30 June 2014)

particular case and the individual citizen, which is perceived as an important aspect of the protection of individual rights. More generally, the one-stop-shop principle was seen as benefitting multinational business at the expense of individual citizens.

This interpretation of the one-stop-shop principle paints an unduly negative picture of the proposals currently on the table. Indeed, it is possible to reconcile the principle with a high standard of protection for citizens' fundamental rights, including those protected by Article 47 of the Charter. This position is based on a number of considerations.

First and foremost, it is important to underline that at present, pursuant to Article 28(6) of Directive 95/46/EC, a DPA is always competent to exercise its powers, including those with regard to the investigation of complaints, within the territory of its own Member State. However, unless the complaint concerns a controller (or a processor) with an establishment or equipment in that Member State, the effective powers of that DPA to enforce the data protection law may in practice be limited. Indeed, the necessity to apply, in a specific case, the national law of a different Member State and the lack of possibilities to conduct investigations or to impose sanctions where there is no physical presence of the controller or processor may render the recourse to the local DPA purely theoretical and largely ineffective.

In contrast, the proposed Regulation would ensure a uniform legal framework and put in place different mechanisms to ensure effective enforcement in practice. Citizens would be explicitly given the right to lodge a complaint with the local DPA or any other DPA in order to exercise their rights.[191] In practice, the local DPA will probably function as the one-stop-shop for citizens in that jurisdiction. However, in cases where today a DPA would have limited options, the new Regulation would ensure effective enforcement by the lead authority in the context of the one-stop-shop for companies (and with the support of the consistency mechanism), and where necessary with the involvement of the locally competent DPA. In addition, affected individuals will always have the possibility to bring legal proceedings against a company established in their country before their national courts for an alleged violation of the Regulation.[192]

From this perspective, the Regulation will have a very positive impact on the possibilities for individuals to enforce their data protection rights, and thus bring about a significant improvement for data subjects in their right to an effective remedy as guaranteed under Article 47 of the Charter.

The Regulation also provides for review of decisions taken by a DPA by the courts. In cases where the one-stop-shop principle applies, an individual wishing to challenge a decision

[191] Article 73
[192] Article 75

taken by the lead DPA would have to do so before a court in the Member State of the lead DPA[193], which in many cases would in practice mean having to initiate legal proceedings in another Member State.

In this context, the sole fact that courts in a Member State other than the country of residence of a citizen must be called upon, does not in itself deprive that citizen of effective judicial protection. Under the current Directive 95/46/EC it is also possible that citizens who wish to complain about the processing of personal data by a company operating in numerous Member States must address themselves to one specific DPA and, if they wish to contest its decisions, must pursue litigation in that same Member State. So far, there has been no reason to call this feature of the current system into question with the Charter.

The proposed one-stop-shop principle is also criticised for creating excessive obstacles for citizens seeking judicial remedies due to geographical distance involved, unfamiliarity with a foreign legal system, the need to initiate and conduct proceedings in a foreign language, or the costs of such a procedure.

The alternative solution proposed in that respect appears to be the creation of an EU body with legal personality which would play the role of the one-stop-shop, both for citizens and for companies. This would require a fundamental centralisation of the existing de-centralised structure of data protection supervision, which would not necessarily facilitate the decision making process within a reasonable time limit, and would certainly not ensure more 'proximity' for citizens and companies alike. More importantly, it does not seem necessary to ensure a better protection of fundamental rights of citizens.

It is important to keep in mind that in most cases all relevant actors - data subjects, controller and DPA - will continue to reside in one country. Consequently, the one-stop-shop principle for companies would only apply in a relatively limited number of situations. It might further be possible to exclude issues of a predominantly local nature, such as issues arising under local laws. In other words, although some of the remaining cases may have large impact, the instances in which citizens are affected by decisions of a lead DPA located in a Member State other than their own country of residence would in practice be much less numerous than the 'ordinary' cases in which decisions are taken by the 'home' DPA.

Finally, the one-stop-shop principle for companies must be seen in its proper context as an important element contributing to the overall effectiveness and consistency of the future data protection framework. Undoubtedly, a much more uniform data protection system and reduced litigation costs - as litigation would in principle be limited to the jurisdiction of the lead DPA or the main establishment - would be advantageous for business across the EU.

[193] Article 74 (3)

However, citizens will also benefit from more consistent application of a uniform set of data protection rules under the proposed Regulation.

For instance, where a citizen is affected by data processing by a controller established in different countries, but all decisions are effectively taken by the main establishment of the controller in another Member State, the possibility to obtain a single decision of a DPA or a court ruling which would be valid and enforceable in all Member States would constitute a considerable improvement compared to the current situation.

By the same token, the one-stop-shop for companies also reduces the likelihood of parallel proceedings and the resulting conflicts of jurisdiction, since a procedure in the Member State of the lead authority would normally be sufficient to enforce one's rights across the EU.

As this discussion illustrates, the one-stop-shop concept, either for companies or citizens, gives rise to questions which may require some fine tuning of the proposed Regulation. This is why different options are still being considered. However, it is clear that the outcome will be based on close cooperation between authorities rather than on exclusive competences, while the need for effective protection and greater efficiency will no doubt also be given adequate weight.

D. More Global Privacy and 'Interoperability'

The digital environment has increasingly a global character, as the Internet and other global networks allow data to move around the world every moment of every day. The international dimensions of the Regulation have therefore also received considerable attention.

In this context, the Regulation - as Directive 95/46/EC, but even more so – does not primarily focus on *where* the data are, but rather on the *responsibility* for the data processing and the *impact* of the data processing on the data subjects. This is most obvious in the scope of the Regulation, which will apply not only to all processing in the context of an establishment of the controller in the EU, but also when goods or services are offered on the European market, or the behaviour of data subjects in the EU is monitored, regardless from where.[194] In all those situations, the controller will be responsible for compliance with the basic principles of

[194] See Article 3. The CJEU has recently ruled in *Google Spain* (see footnote 45) that Directive 95/46/EC already applies to a search engine operating from a third country via its subsidiary in an EU Member State. In this respect, the Court ruled that the search engine operator was a controller as regards the processing of personal data carried out by the search engine and that the activities of the subsidiary - although limited to the sales of advertising - were inextricably linked to the processing of personal derived from searches which made the advertising more valuable (see *Google Spain*, at 33 and 55-56). In this way, the Court has taken an important step in the direction also aimed at by the Regulation.

data protection and the rights of the data subject, and be subject to the control of independent supervisory authorities.[195]

To the extent that the Regulation applies, it will also require that personal data are not transferred to a third country, unless that destination ensures an adequate level of protection, or adequate safeguards are provided by other means. Those provisions have been elaborated and simplified, so that there will be more options to provide adequate protection in specific situations.[196] The underlying idea is that personal data should only be transferred to a third country, if the rights of data subjects are safeguarded. At the same time, these provisions are based on a reasonable degree of pragmatism in order to allow interaction with other parts of the world. They will therefore also apply if personal data are transferred to service providers in third countries in the context of cloud computing. In those cases, the controller will remain at least co-responsible for compliance with data protection requirements.[197]

A third element is that the Regulation will also encourage cooperation with data protection authorities in other parts of the world.[198] This is important to effectively deal with global actors on the Internet. As already highlighted in Section 5, Part C, this development benefits from a growing convergence of data protection principles and practices around the world, and is encouraged by the partly overlapping frameworks of the Council of Europe and the OECD.

The OECD has recently published revised Privacy Guidelines, which basically confirm the approach followed so far.[199] The revised Guidelines also emphasize the need for practical measures to ensure compliance with data protection principles, and the need for cooperation of privacy enforcement authorities.[200] The revision of Convention 108 of the Council of Europe goes in a similar direction.[201]

---

[195] In its ruling the Court observed that the controller must ensure - within the framework of its responsibilities, powers and capabilities - that its activity complies with the requirements of the Directive (see *Google Spain*, at 38). This also applies where this activity is performed by computers on the basis of computer programmes: a welcome endorsement of the responsibility of controllers and the scope of their obligations on the internet. A key consideration of the Court is the need to ensure 'effective and complete protection' to fundamental rights (*Google Spain*, at 34, 38, 53 and 58). An important detail is that the Court again confirmed that the Directive applies to personal data which have been published (*Google Spain*, at 30). In determining the rights of the data subject under Articles 12 and 14 of the Directive - notably the right to erasure and the right to object to processing of personal data - the Court specifically referred to Articles 7 and 8 of the Charter (*Google Spain*, at 69, 81 and 97). The ruling can therefore also be seen as further evidence of the growing impact of the Charter on the application of existing law.

[196] Articles 40-44

[197] Article 24

[198] Article 45

[199] Available at http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines (last accessed 31 May 2014)

[200] Part Three on 'Implementing Accountability' and Part Six on 'International Cooperation and Interoperability'

[201] See information available at http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp (last accessed 31 May 2014)

All these elements together will allow a gradual development towards global 'interoperability' of privacy and data protection frameworks. Although it would be fairly easy to identify many differences of detail, there is also a growing scope for synergy and convergence among those frameworks. The Regulation would be the most developed framework in the world - in line with the recognition of the right to data protection as a fundamental right in Article 8 of the Charter - but it would also be consistent with developments elsewhere. Moreover, it may well have a strong influence on those developments in due course, much like Directive 95/46/EC exercised in the past. The review of the Directive therefore also offers a major opportunity to ensure more global privacy and interoperability.

Finally, the Regulation does not apply to surveillance activities undertaken by third countries or by the relevant services of an EU Member State. However, it does apply to operators and other services providers which offer their services on the European market or monitor the behaviour of data subjects in the EU, and may thus also provide opportunities for spying by other actors.[202] The controller's obligations under the Regulation would in this respect serve as an important countervailing power.

Against this background and in a wider context, it would be helpful if the Regulation would also contain a provision addressing the situation where a legal obligation imposed by a third country would require activities which are not in conformity with EU law.[203] In principle, such activities should not be allowed, except where an international agreement would allow them or an independent judicial or supervisory authority would have granted an exemption. Such a provision could serve as a necessary regulator in cases where international conflicts of law or public policy could otherwise only go at the expense of economic operators or general interests and possibly both.

7. Other Issues

A. Internal Market and Fundamental Rights

Directive 95/46/EC has been adopted on an internal market legal basis in order to provide a harmonised legal framework for data protection in the EU. However, the fundamental rights perspective has been visible from the beginning. The Court of Justice has highlighted that the Directive has a very broad scope and the Charter has a growing impact on its application in practice. The review of the Directive is now taking place in a different perspective. Article 16 TFEU has provided a general legal basis for comprehensive protection of personal data in all

[202] Article 3

[203] Such a provision was part of the Commission proposal for the Regulation before it was deleted at a late stage. The Parliament and the Council are also considering different versions of a similar provision. Its benefits would go beyond surveillance and could also involve other areas where international conflicts of law or public policy might arise, typically including legal obligations requiring access to information in other jurisdictions.

policy areas and the Charter applies to the EU institutions and the Member States whenever they act within the scope of EU law.

This different perspective does not mean that internal market considerations and other public policy principles could no longer play a role in the way in which the review of the current EU legal framework for data protection is undertaken, and indeed in the structure and the content of the new legal framework itself. It is obvious that the choice for the proposed Regulation and many of its main features are based on the need for greater harmonisation to provide stronger, more effective and more consistent protection of personal data across the EU. In other words, the impact of the Charter and the need for harmonisation and consistency across the EU are not only compatible and complementary, they are mutually reinforcing. Strong and consistent data protection is also in the interest of the internal market.

However, one could still raise the question how much flexibility Article 16 TFEU allows and where the impact of the Charter might pose certain limits which public policy developers and the EU legislator have to respect. This is not a purely theoretical question as the discussion in the Council about the one-stop-shop for companies has highlighted.[204] Legal objections to the one-stop-shop principle have been raised to question its compatibility with the Charter and in particular with Article 47 on the right to an effective remedy and a fair trial. Although these objections are not fully convincing, they suggest that there are indeed different limits which the EU legislator has to respect.[205]

The Court of Justice has also demonstrated that such limits exist. The clearest example of this is the case law on the requirement of 'complete independence' for supervisory authorities. On various occasions, the Court has stated that the requirement of independent supervision is an 'essential component' of the protection of personal data, and also derives from Article 8(3) of the Charter and Article 16(2) TFEU.[206] This means that the EU legislator would not be free to revise the current framework in a way which would not be compatible with those provisions of primary law.

Something similar could be deduced from the recent ruling of the Court about the position of search engine operators. As the scope of the data subject's right to erasure and to object to processing of personal data, under the current Directive, were set out with specific references to Articles 7 and 8 of the Charter[207], it would be inconceivable to limit the scope of those

[204] See supra Section 6, Part C
[205] See also, in a different context, *Digital Rights Ireland* (footnote 97), at 47: "With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference".
[206] See footnote 95
[207] See footnote 195

rights without due regard to the requirements in the Charter for any limitation on the exercise of the rights explicitly recognised in Article 8(2) or implicit in Article 8(1) of the Charter. The Court came indeed very close to saying that these rights are (also) 'essential components' of the protection of personal data under Article 8. The same might happen in future cases about other parts of Article 8.

More in general, this means that Articles 7 and 8, as well as other relevant provisions of the Charter have to be kept in mind when the details of the Regulation are discussed and adopted, and eventually applied in practice. It is here that the difference in character between the rights to respect for private life and the right to the protection of personal data may once again play an important role. Article 7 would then primarily serve as a guard against undue interferences with the private life of individuals, while Article 8 would serve as a positive guarantee that the essential elements of the protection of personal data, as set out in this provision, are delivered adequately in practice.

This implies that the Regulation should be designed and applied in such a way, that the processing of personal data, either by public or private actors, does not amount to an undue interference with the private life of individuals, and that the essential elements of data protection are provided both in the public and in the private sector. Any reduction in the scope or the level of protection under the current Directive might therefore well face justified challenges under Article 7 and 8 of the Charter.

B. Accountability and Compliance

In Section 5, parts B and C, we mentioned that one of the most important elements of the Regulation is the shift from prior control to ex-post control by data protection authorities and from nominal responsibility to enhanced responsibility or accountability for controllers. One commentator has referred to this shift as a 'Copernican revolution in European data protection law'.[208] Although this terminology may be overstated, it certainly underscores a major change of approach with a view to making data protection more effective in practice.

It is important to further clarify what this shift entails. First of all, it does not change the existing responsibility of controllers to ensure compliance with the substantive principles of data protection and certain specific rights of data subjects. All these essential elements will remain unaffected, subject to some clarifications and improvements in the Regulation.

In the current Directive, this is complemented by a general obligation for prior notification of data processing operations to the competent DPA, which may be subject to exemptions, or by an obligation for prior checking in the case of risky processing operations.[209] In practice, this

[208] See C. Kuner (footnote 128)
[209] Articles 18-20

has not only led to very great diversity among the Member States, both as to the scope for notification or exemption, and with regard to the national practices under each of the relevant categories. More importantly, responsible organisations are inclined to see formal notification as the main obligation, rather than the obligation to comply with data protection principles. This has put undue emphasis on the role of data protection authorities at the expense of the key role of controllers to provide good data protection in their organisations. The obligation to prior notify individual processing operations is now widely perceived as an ineffective and unnecessary administrative burden.

Instead, the Regulation has put more emphasis on the responsibility of controllers. As a result they will not only have to comply with substantive principles and data subject's rights, but also to take all appropriate measures to ensure compliance, and to verify and demonstrate that those measures exist and continue to be effective. [210] This principle of accountability should lead to better *data management* in practice, subject to the 'progressive' risk-based approach, as referred to in Section 6, part B. The powers of data protection authorities to enforce, and to impose sanctions for non-compliance, have also been increased substantially.[211]

The separate obligation to take appropriate measures and to demonstrate their existence and continued effectiveness is designed to work as an incentive for controllers and a tool for data protection authorities to supervise data management practices, without necessarily having to go into time consuming analysis of substantive issues. A 'progressive' risk-based approach, as mentioned above would work well in this context, both for controllers and for data protection authorities. This will also require some practical guidance from those authorities, preferably in the context of the European Data Protection Board, so as to ensure sufficient consistency across the EU.

It is not difficult to predict that controllers will be inclined to seek expert advice on how to best ensure compliance in their organisations. This will lead to a growing demand for privacy professionals and privacy relevant products and services, possibly subject to certification on the basis of the Regulation.[212] On the other hand, the Regulation will provide for a more diverse menu of options for enforcement, ranging from individual or collective actions by interested parties, to different interventions by data protection authorities, either or not in the context of a one-stop-shop, backed up by the consistency mechanism and the role of the European Data Protection Board. In other words, controllers will be able to carry their responsibilities, where necessary with the help of others, and may be the subject of different enforcement actions, depending upon whether they are more or less successful.

[210] Article 22
[211] Articles 53 and 79
[212] Article 39

In this way, the Regulation will lead to a better allocation of responsibilities and create some powerful incentives for compliance, which are likely to result in more effective protection in practice.

C. Independent Supervision and Consistency

The requirement of independent supervision has been mentioned above repeatedly as an 'essential component' of the right to data protection, and the need for greater consistency has also been mentioned as a condition for greater effectiveness of that right across the EU. But are these requirements fully compatible with each other? At first sight, this may well be a true paradox in the governance of EU data protection.

According to the case law of the Court of Justice, the requirement of 'complete independence' for a supervisory authority means that it should be free from *any* external influence.[213] This does obviously not exclude that those authorities may cooperate with each other and may develop a consensus on certain issues. However, in case of disagreement, the question of who is to take a binding decision is bound to raise difficult issues. If a minority would be bound by the views of a majority, this would amount to direct external influence and hardly be compatible with complete independence. If on the other hand, each supervisory authority would be free to follow its own views, it would be impossible to achieve real consistency on any subject.

It should be noted that the consistency mechanism in the proposed Regulation would not lead to a binding decision, but result in an *advisory* opinion, in the light of which the competent DPA would have to reconsider its position.[214] If the advisory opinion is followed, there would be no problem. If the competent DPA would disagree, there are in theory two main options.

The first option is that the competent DPA would have to motivate its position and explain why it does not follow the advisory opinion. This would no doubt lead to closer scrutiny of the measure by interested parties and any subsequently involved court. This option would fully respect independence, only create procedural pressure, but possibly also lead to very limited consistency, perhaps only after a final decision of the Court of Justice.

The second option is that the consistency procedure would enter a new phase. In that context, the Commission had envisaged an increasingly active role for itself, first by submission of an opinion, which would require the competent authority to reconsider its position even more seriously, secondly by suspension of the contemplated measure, and finally settling the matter more generally in a binding way by adoption of an implementing act.[215] This approach has

[213] See footnotes 51 and 52
[214] Article 58
[215] Articles 59-62

been widely criticised as inappropriate. Although the Commission is also required to act with full independence according to the Treaties[216], this requirement has a different aim and would not be sufficient to justify a direct intervention in a case before an independent authority.

This state of play has encouraged a rethink of how independent authorities might cooperate in reaching good and consistent outcomes. It has been suggested that issues which are purely or predominantly local in nature - with all actors residing in one country or issues arising under local laws - should be left entirely to locally competent data protection authorities. If more than one jurisdiction is involved - either because the controller has establishments in different jurisdictions or individuals in different jurisdictions are affected - then the first rule should be that the competent authorities should cooperate in reaching a solution of the issue which can be supported by all. In this context, there might be a good reason to designate a lead authority also in cases where a controller is established in only one jurisdiction, while individuals in more jurisdictions are affected. Indeed, it may be that the controller has no establishment at all in the EU and individuals in all Member States are affected. Different scenarios for the designation of such a lead authority could therefore be envisaged. However, as long as the outcome of the cooperation is reached by consensus within a reasonable time, there will be no problem with independence.

If the cooperation between the data protection authorities involved does not lead to consensus within a reasonable time, the issue should be 'pushed up' for discussion by the European Data Protection Board. If the outcome of that discussion is adopted by consensus, there will again be no problem with independence. However, if a majority prevails, there are basically two scenarios. The first one is that the majority view would only be an *advisory* opinion, which the competent DPA should at least consider very carefully. In case of continued disagreement there would be the possibility for a second advisory opinion which should have to be adopted with a qualified majority. This would follow the approach of increasing procedural pressure, without limiting the decision making power of the competent DPA. It would also build on the assumption that a second advisory opinion would be very influential, but without completely deciding all details of a case.

The second scenario would introduce a decision making mechanism at a different level, for instance in the context of the European Data Protection Board itself. This option might also have consequences for the judicial review of any decisions, and might result in an undesirable centralisation. Other possible solutions have also been suggested, however without being able to fully address the problem of a dissenting minority and a possible lack of consistency.

This explains that the governance issues relating to the consistency mechanism, together with the architecture of the one-stop-shop for companies, are among the most complicated issues

[216] Article 17(3) para. 3 TEU

currently still under discussion, and that different solutions are being analysed in order to find an acceptable compromise.

8. Concluding Remarks

The outcome of the current review of Directive 95/46/EC - and of the EU legal framework for data protection more in general - is not yet entirely clear, but its main direction now seems irreversible and well beyond the point of no return. In any case, a few conclusions may be drawn at this stage.

Privacy and data protection - more precisely: the right to *respect* for private life and the right to the *protection* of personal data - have important connections. They are both fairly recent expressions of a universal idea with strong ethical dimensions: the dignity, autonomy and *unique value* of every human being. However, there are also crucial differences. The concept of 'data protection' was developed in order to provide structural legal protection to individuals against the inappropriate use of information technology for processing information relating to them, *regardless* of whether that processing would be within the scope of the right to respect for private life or not. The resulting set of safeguards - in essence a system of checks and balances, consisting of substantive conditions, individual rights, procedural provisions and independent supervision - applies in principle to all processing of personal data.

This approach was developed by the Council of Europe in Convention 108 and further developed by the EU in Directive 95/46/EC, alongside the right to respect for private life as set out in Article 8 ECHR. Both must be distinguished from, on the one hand, the German concept of 'informational self-determination', with a strong emphasis on the data subject's consent, and on the other hand, the approach followed by the OECD Guidelines, based on the notion of 'risk' as a *threshold* condition for protection, and assuming that all processing of personal data is in principle legitimate. These distinctions play an important - but often only implicit and insufficiently recognised - role in international discussions.

The EU has gradually taken over the role of the Council of Europe as a building platform for data protection. In this respect, we have seen two lines of development: the first having to do with making privacy and data protection rights *stronger*, and the second with ensuring a more *consistent* application of those rights across the EU. Both lines aim to ensure *more effective* protection in practice and less *unhelpful diversity* in the way this protection is delivered in the Member States. The increasing impact of the Charter of Fundamental Rights, both in the case law of the Court of Justice and in the review of the current legal framework, is in accordance with this long term trend. This is obviously very welcome, as the need for effective protection of personal data has never been greater than today.

The distinction between 'privacy' and 'data protection' is also relevant for the Charter. Article 7 on the right to respect for private life is a typical example of a classical fundamental right, where *interference* is subject to strict conditions. Article 8 on the protection of personal data follows Convention 108 and Directive 95/46/EC in providing a system of more pro-active protection. This means that the *scope* of Article 8 - involving all processing of personal data - should not be confused with the question whether the fundamental right to data protection has been *interfered* with. Such interference normally only happens if one or more of the main components of Article 8(2) and 8(3) have not been respected. However, it should not be excluded that Article 8(1) might serve as a source of other requirements, already set out in EU data protection law, but not yet made explicit in the Charter.

In its recent case law, the Court of Justice shows a tendency towards a 'combined reading' of Articles 7 and 8 of the Charter. As we have explained, this approach does not take account of the essential difference in character between the two provisions and may prevent Article 8 from reaching its full potential. However, the Court still seems to be struggling with the proper role of Article 8 Charter and it sometimes uses different terminology.

The general basis for the review of the current legal framework in Article 16 TFEU offers a historic opportunity to deliver the main components of Article 8 Charter in a more effective and consistent set of rules across the EU. The General Data Protection Regulation, which is to replace Directive 95/46/EC in due course, is a combination of continuity and innovation. A directly binding Regulation will in principle bring much greater consistency, but in practice probably also allow some flexibility for interaction with national law, especially in the public sector. The greatest innovation is expected in larger responsibilities for controllers, although the impact of this shift will depend on the 'progressive risk based approach' currently under discussion. Innovation can also be expected in the area of supervision and enforcement, especially in relation to the details of one-stop-shops for citizens and business and in other mechanisms to ensure consistent outcomes of independent supervisory authorities. Finally, the territorial scope of the Regulation is likely to also include companies that are operating on the European market from an establishment elsewhere in the world.

As the Charter is always applicable within the scope of EU law, it will also apply to the legal framework that will eventually be adopted on the basis of Article 16 TFEU. This leads to the question how much discretion the legislature will have in the adoption of those rules. In our discussion, we have seen different examples of a limited discretion, either because Article 8 Charter has already set certain positive requirements, or because the Charter also needs to be respected whenever rules of data processing may serve as a basis for interference with the right to respect for private life. Problems with the Charter might also arise, when the scope or the level of protection of the new rules would be more limited or lower than under the current legal framework.

Finally, we have seen that the governance issues relating to the one-stop-shop for companies and the consistency mechanism are among the most complicated issues that are currently still under discussion. Creativity and pragmatism will both be needed here, in order to ensure that the essential components of Article 8 Charter can be effectively delivered in practice.