scripted

Volume 9, Issue 1, April 2012

A GENERAL DATA PROTECTION REGULATION FOR EUROPE? LIGHT AND SHADE IN THE COMMISSION'S DRAFT OF 25 JANUARY 2012

Gerrit Hornung [*]

Abstract

On 25 January 2012, the European Commission presented the long-awaited proposal for a reform of the European data protection law. The proposal consists of a "General Data Protection Regulation" (replacing the current Data Protection Directive 94/46/EC) as well as a Directive with regard to data processing for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (superseding the Framework Decision 2008/977/JHA). This article gives an overview of the draft Regulation and provides a more in-depth insight into selected issues concerning the scope of application, the rights of the data subject, modern data protection instruments and institutional issues. Overall, the proposal contains a number of commendable provisions but also some points worthy of criticism. The latter are particularly related to national data protection regimes which have specific regulatory traditions and provide for elaborated data protection rules under the current European framework. In this respect, Germany serves as an instructive example.

DOI: 10.2966/scrip.090112.64

 © Gerrit Hornung 2012. This work is licensed under a Creative Commons Licence. Please click on the link to read the terms and conditions.

[*] Professor for Public Law, IT Law and Legal Informatics, University of Passau, gerrit.hornung@uni-passau.de. An earlier version of this paper appeared in German in the Zeitschrift für Datenschutz (ZD) 2012, 99-106 and this version is published with its permission. The author is grateful to Mr Markus Lieberknecht for his support on the revised version.

1. Background

Measured against the innovation cycle of the modern information society, the European Data Protection Directive (EDPD) appears to be an ancient regulatory instrument. The Commission's first proposal dates back to 11 September 1990,[1] ie a point in time when there was no world wide web. The EDPD, adopted on 24 October 1995,[2] contains binding guidelines for the national data protection laws of the Member States, and it is generally believed that it urgently needs to be modernised.[3] The Commission has taken the initiative and issued a Communication regarding "A comprehensive approach on personal data protection in the European Union" in late 2010.[4] The recently published draft of a "Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" (GDPR)[5] carries on with the Communication's concepts of modernisation. Recital 7 correctly points out that, despite the need for revision, the basic objectives and principles of the EDPD remain sound: providing a uniform protection of basic rights with regard to personal data processing as well as ensuring the free movement of such data between Member States. However, technological developments and globalisation make it imperative to revise the current provisions of the EDPD (cf Recital 5 et seq).

The Commission's proposal, which is now based on Art 16 of the Treaty on the Functioning of the European Union (TFEU),[6] is not only concerned with the regulatory scope of the EDPD. The simultaneously issued proposal for a "Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data"[7] is intended to further harmonise this area, which is currently regulated by Framework Decision 2008/977/JHA.[8] The overall strategy is explained

---

[1] C 277 Official Journal of the EU, 5 Nov 1990 3.

[2] *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the movement of such data*, L 281 Official Journal of the EC 23 Nov 1995, 31.

[3] See, *inter alia*, S Simitis, "Die EG-Datenschutzrichtlinie: eine überfällige Reformaufgabe" in F Herzog and U Neumann (eds), *Festschrift für Winfried Hassemer* (Heidelberg, Hüthig-Jehle-Rehm, 2010), 1235-1248. On the parallel process within the Council of Europe see S Kierkegaard, N Water, G Greanleaf, L Bygrave, I Lloyd and S Sayby, "30 years on – The Review of the Council of Europe Data Protection Convention 108" (2011) 27 *Computer Law & Security Review* 223-231.

[4] European Commission, COM(2010) 609 final, 4 Nov 2010.

[5] European Commission, COM(2012) 11 final, 25 Jan 2012.

[6] Concerning the provisions on data protection in the Treaty of Lisbon, see from the German perspective I Spiecker and M Eisenbarth, "Kommt das 'Volkszählungsurteil' nun durch den EuGH? – Der Europäische Datenschutz nach Inkrafttreten des Vertrags von Lissabon" (2011) 66 *JuristenZeitung* 169-177.

[7] European Commission, COM(2012) 10 final, 25 Jan 2012.

[8] L 350/60 Official Journal of the EU, 30 Dec 2008.

in a comprehensive Communication "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century".[9]

A preliminary version of the three texts was leaked in November 2011.[10] Apparently, significant reservations regarding the Commission's approach emerged within the data processing economic sector and during the consultations with the United States. In an "informal note", the US administration particularly criticised the introduction of new protection instruments (data breach notification, right to be forgotten, protection of children's data), the regulation of data transfers to third countries, and the requirement to obtain the authorisation of the competent supervisory authority prior to any disclosure of personal data upon the request of courts or authorities of third countries (Art 42 (2) of the draft).[11] The impact of this criticism cannot be determined from the outside. Certainly, the version that was eventually adopted differs from the November 2011 draft in some important aspects. This includes especially the age of consent for children, which has been lowered from 18 to 13 years (Art 8 (1) GDPR; this corresponds with US legislation) as well as the deletion of Art 42 of the draft (a weakened provision is now contained in Recital 90).

2. The Change to a Regulation

The proposed change to the instrument of a Regulation bears both symbolic value and extensive legal implications. Symbolically, the change represents the Commission's view that the EDPD did not lead to a sufficient harmonisation of data protection law within the Union (Recital 7) as well as the hope for an enhanced unification of law and more legal certainty in order to strengthen the rights of data subjects and promote a single market without obstacles for the free movement of data (Recital 11). Legally, the change of instrument entails that the new provisions would be binding in their entirety and thus have direct effect in all Member States when adopted pursuant to Art 288 (2) TFEU. National courts and authorities would not resort to their respective data protection laws but directly apply the provisions of the GDPR which the European Court would be competent to interpret under the preliminary ruling procedure (Art 267 (1) (b) TFEU).

In light of these implications, *Johannes Masing*, the judge responsible for data protection issues at the German Federal Constitutional Court

---

[9] European Commission, COM(2012) 9 final, 25 Jan 2012.

[10] Statewatch, "Observatory on Data Protection in the EU" (2012), available at http://www.statewatch.org/eu-dp.htm (accessed 28 Feb 2012).

[11] European Digital Rights (EDRi), "US Lobbying Against Draft Data Protection Regulation" (2011) available at http://www.edri.org/US-DPR (accessed 28 Feb 2012). The requirement to obtain authorisation would have concerned especially the area of so-called "e-discovery", see eg D B Garrie and M Duffy-Lewis, "Conquering the Tower of e-Discovery Babel: New Age Discovery for the 21st Century" (2009) 6:1 *SCRIPTed* 121. On the possible conflicts with European data protection law see Article 29 Data Protection Working Party, "Working Document 1/2009 on Pre-trial Discovery for Cross Border Civil Litigation" available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf (accessed 28 Feb 2012); on the German perspective eg K Brisch and P Laue, "E-Discovery und Datenschutz" (2010) 26 *Recht der Datenverarbeitung* 1-7; H Özbek, "Datenschutzkonformer Einsatz von E-Discovery Systemen" (2010) 34 *Datenschutz und Datensicherheit* 576-580; Judgement by District Court of Utah with comments by A Spies and C Schröder, "Deutsches Datenschutzrecht blockiert nicht die US-Beweiserhebung (E-Discovery)" (2010) 13 *Multimedia und Recht* 275-277.

(*Bundesverfassungsgericht*), has expressed fundamental criticism of the Commission's proposal.[12] Due to the supremacy of European Law, the basic rights of the German Basic Law (*Grundgesetz*), as well as respective national provisions of other Member States, would indeed cease to be applicable within the scope of the GDPR, which would limit the jurisdiction of the national constitutional courts accordingly.[13] With regard to data processing carried out by non-public parties, this concerns classic issues of balancing personal rights and other fundamental rights (e.g. freedom of expression). Since the GDPR covers public administration with the exception of prevention and prosecution of crimes, another area of sovereign data processing would cease to be under the control of the national constitutional courts. As for the German example, this would most notably cover the case of the national census and would have prevented the *Bundesverfassungsgericht* from inventing its famous "right to informational self-determination"[14] in a decision on this matter.[15]

This shift is important for two reasons: first, there is no remedy available to individuals on a European level that is comparable to the German *Verfassungsbeschwerde* or other national constitutional complaint. Moreover, despite its expanded case law on fundamental rights, the European Court is still a long way from developing and applying consistent fundamental rights mechanisms comparable to those developed by the European Court of Human Rights, the *Bundesverfassungsgericht* and many other national constitutional courts.[16] For reasons of the limited resources of the European Court alone this will hardly change in the future. Arguably, the only way to establish a specific control mechanism for fundamental rights on a European level would be the succession of the Union to the European Convention on Human Rights, which continues to be delayed and could also add to the overload of cases the European Court of Human Rights has to deal with already.

In the German discussion, there are several voices that call for a split of the regulatory instrument. While it is largely accepted that a regulation is the appropriate choice for the private sector, it is frequently questioned whether data processing in the public sector needs the same degree of harmonisation. The Federal Council of Germany (*Bundesrat*) has thus emphasised its opinion that the proposal is in conflict with the principle of subsidiarity (Art 5 (3) TEU).[17] This obviously reflects the concern of national parliaments that they might lose their influence in this important area, but it

---

[12] J Masing, "Ein Abschied von den Grundrechten" (2012) 9 January *Süddeutsche Zeitung*.

[13] See eg N Matz-Lück, "Europäische Rechtsakte und Nationaler Grundrechtsschutz" in N Matz-Lück and M Hong (eds), *Grundrechte und Grundfreiheiten im Mehrebenensystem – Konkurrenzen und Interferenzen* (Heidelberg: Springer, 2012) 161-201.

[14] Bundesverfassungsgericht, decisions volume 65, 1 et seq; G Hornung and C Schnabel "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-determination" (2009) 25 *Computer Law & Security Review* 84-88.

[15] Further possible examples include the financial administration (regarding the access of bank account master data, see Bundesverfassungsgericht, decisions volume 65, 118, at 168) or right to access to personal data in government files (eg Bundesverfassungsgericht, decisions volume 120, 351). The author is grateful to Matthias Bäcker, University of Mannheim, for his views on this point.

[16] Regarding the data protection judicature of the ECJ, see eg R Streinz, "Die Rechtsprechung des EuGH zum Datenschutz" (2011) 35 *Datenschutz und Datensicherheit* 602-606.

[17] See Bundesrat Printed Paper 52/12(B).

is also true that the current proposal could even out the different data protection requirements in several specific public areas in Germany, e.g. in the social security sector. Different national data protection rules in these areas will also hardly have negative impacts on the common market.

Regarding substantive law, the change to a Regulation would first of all render the dispute on the full or minimum harmonisation of the current EDPD obsolete.[18] Further, national legislators would – especially in light of the extensive competences of the Commission to adopt delegated acts – largely be precluded from adopting specific provisions to concretise general data protection principles. In Germany, this would lead to significant changes. Specific rules for video surveillance or chip cards as in §§ 6b, 6c of the Federal Data Protection Act (*Bundesdatenschutzgesetz*) would be impossible.[19] Instead of the limit set forth in § 4f (1) *Bundesdatenschutzgesetz* (ie employing at least ten persons in the automated processing of personal data), Art 35 (1) (b) GDPR would impose a general duty to appoint a data protection officer only for companies with 250 employees or more. The general German requirement that consent must be expressed in written form (§ 4a (1) 2nd sentence *Bundesdatenschutzgesetz*) could not be upheld as it contradicts Art 4 (8), Art 6 (1) (a) and Art 7 GDPR. Last but not least, the development of innovative regulatory instruments to protect personal data would be rendered impossible on the national level. This appears to be undesirable when taking into account that the proposal picks up developments that emerged precisely from the national leeway left by the EDPD, namely as regards data protection by design and by default (Art 23 GDPR) as well as auditing and reviewing procedures (Art 22 GDPR).[20]

Whereas some observers from Germany and other Member States with a strong data protection tradition may thus tend to consider the GDPR a step backwards, the Commission's motives are understandable when examining the current state of data protection law in practice. The EDPD has led to a certain level of formal harmonisation. However, there is a wide range of different approaches in national legislation, and the actual level of protection varies considerably.[21] This is aggravated by the fact that national supervisory authorities interpret their role differently and have unequal resources they can resort to. Consequently, the European Data Protection Supervisor has welcomed the Commission's approach in this respect.[22]

The draft contains only a few opening clauses. According to Art 80 GDPR, Member States shall provide for exemptions or derogations for the processing of personal data carried out solely for journalistic, artistic or literary purposes. Specific rules can also be adopted for processing of personal data concerning health (Art 81 GDPR) and for

---

[18] The ECJ regards the EDPD as a "harmonisation which is generally complete", see Lindqvist v Sweden [2003] C-101/01 (ECJ), para 29; Huber v Federal Republic of Germany [2008] C-524/06 (EJC); Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) v Administración del Estado [2011], joined cases C-468/10 and C-469/10 (ECJ), para 29; in the last case, the ECJ also affirmed the direct effect of Art 7 (f) EDPD.

[19] This is also one concern of the German Bundesrat, see Bundesrat Printed Paper 52/12(B) at 2.

[20] See further G Hornung "Datenschutz durch Technik in Europa" (2011) 1 *Zeitschrift für Datenschutz* 51-56.

[21] See the evaluation report of the Commission contained in the annex to SEC(2012) 72 final.

[22] See European Data Protection Supervisor, "Opinion on the Data Protection Reform Package", 7 March 2012, para 18.

"regulating the processing of employees' personal data in the employment context" (Art 82 GDPR). Regarding Germany, the latter is thus referred back to the national legislator, which has remained largely inactive since the hearing by the Federal Parliament's interior committee on 23 May 2011.[23] Furthermore, opening clauses exist concerning in particular the basis of the processing (Art 6 (3) (b) GDPR), the regulation of processing of specific categories of personal data (Art 9 (2) (b), (g) GDPR), exceptions from the right to be forgotten and from the prohibition of measures based on profiling (Art 17 (3) (d), Art 20 (2) (b) GDPR), restrictions of the rights and obligations due to certain public interests (Art 21 GDPR), the modes of establishing supervisory authorities (Art 46, 48 GDPR), the right to bring representative actions (Art 73 (2) GDPR), and obligations of secrecy (Art 84 GDPR).

3. Overview of Structure and Content

The draft consists of eleven chapters. The general provisions (chapter 1) set forth objectives, definitions, as well as the material and territorial scope. Some definitions are adopted from Art 2 EDPD, others originate from different EU Directives or have not yet been legally defined in data protection law (genetic and biometric data, data concerning health, group of undertakings, main establishment, etc.). The terms "personal data" and "data subject" are defined separately, but together they still correspond with the present criteria of identified or identifiable persons. Recital 23 adheres to the approach that in order to determine whether a person is identifiable "account should be taken of all the means likely reasonably to be used whether by the controller or by any other person to identify the individual".

Chapter 2 determines general principles, some of which correspond with Art 6 EDPD, while others exceed this provision (in particular regarding the principles of transparency and data minimisation, as well as the comprehensive responsibility of the controller). With some modifications, Art 6 GDPR matches Art 7 EDPD (especially regarding the requirement of a specific legal basis for every processing of personal data).[24] This is followed by conditions for consent (Art 7 GDPR), the processing of personal data of children (Art 8 GDPR) and the processing of special categories of personal data (Art 9 GDPR, now extended to genetic data and data concerning criminal convictions or related security measures, while not including biometric data).

The rights of the data subject (Chapter III) are substantially broadened and regulated more precisely than in the EDPD. Along with general provisions concerning transparency (Art 11 GDPR et seq.), the draft contains the established rights to information, access, rectification, erasure and object (Art 14 GDPR et seq.). The right not to be subject to a measure based on profiling (Art 20 GDPR) extends Art 15 (1) EDPD. The right to be forgotten (Art 17 GDPR, which is however based on the right to erasure) and the right to data portability (Art 18 GDPR) are new additions. Art 21

---

[23] See the draft legislation submitted by the German Federal Government (Bundestag Printed Paper 17/4230), the Social Democratic Party (SPD) (Bundestag Printed Paper 17/69) and by the Green Party (BÜNDNIS 90/DIE GRÜNEN) (Bundestag Printed Paper 17/4852).

[24] In the current German debate, there are voices which call for the abolition of this principle, cf J Schneider "Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip" (2011) 61 *Anwaltsblatt* 233-239; J Schneider and N Härting " Warum wir ein neues BDSG brauchen - Kritischer Beitrag zum BDSG und dessen Defiziten" (2011) 1 *Zeitschrift für Datenschutz* 63-68.

GDPR, modelled after Art 13 EDPD, contains powers for Union and Member States to restrict the scope of several obligations and rights by way of legislative measures.

The provisions concerning controllers and processors are laid out in a more detailed manner as well (Chapter IV). Picking up on some points that were brought up in the discussion on the principle of accountability,[25] they are summarised in Art 22 GDPR and subsequently specified with regard to particular duties; this includes the duty to cooperate with the supervisory authority (Art 29 GDPR) and requirements for the security of processing (Art 30 GDPR). The general duty to notify the supervisory authority under Art 18 (1) and Art 19 EDPD is repealed and gives way to a duty of controllers and processors to document all processing operations (comprehensively regulated in Art 28 GDPR). There are several new points included, namely the duties with regard to data protection by design and by default (Art 23 GDPR), the responsibility of joint controllers (Art 24 GDPR), the duty to notify in case of a personal data breach (Art 31 GDPR et seq.), the obligation to carry out data protection impact assessments under certain circumstances (Art 33 GDPR) as well as the possibility to introduce certification mechanisms, data protection seals and marks (Art 39 GDPR). The proposal deals with processors in far more detail than the current EDPD (Art 26 GDPR et seq.). Art 35 GDPR makes the designation of an internal data protection officer mandatory instead of optional, as provided by the current Art 18 (2) EDPD. However, this only applies where data is processed by a public authority or body or by an enterprise that either employs 250 persons or more or whose "core activity" consists of "processing operations which, by virtue of their nature, their scope and/or their purposes require regular and systematic monitoring of data subjects".[26] Moreover, the Commission is authorised to adopt implementing acts for deciding that codes of conduct submitted to it have general validity within the Union (Art 38 GDPR).

The rules concerning data transfer to third countries or international organisations (Chapter V) contain a number of permitted transfers. Accordingly, the transfer may be permissible on the basis of an adequacy decision of the Commission (Art 41 GDPR) or appropriate safeguards (in particular by standard data protection clauses, binding corporate rules, and contractual clauses, cf Art 42 GDPR et seq; the Commission may declare standard data protection clauses generally valid). Additionally, Art 55 GDPR provides for derogations (for instance in case of informed consent, on "important grounds of public interest", and for the purpose of legitimate interests which "cannot be qualified as frequent or massive").

The provisions that deal with supervisory authorities are noticeably more elaborate than in the current framework (Chapter VI). Besides the duty to establish such authorities (Art 46 GDPR), the draft states their independence more precisely (Art 47 GDPR) and establishes a codification of their competences, duties and powers (Art 52 GDPR et seq., in particular the power to sanction administrative offences), which are currently applied very differently in the Member States. The concept of a (single) competent supervisory authority at the place of the main establishment (so-called principle of a "one-stop shop") in Art 51 GDPR is completely new.

---

[25] See eg Article 29 Data Protection Working Party, "Opinion 3/2010 on the Principle of Accountability" (2010) available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (accessed 28 Feb 2012).

[26] See 4.4 below.

Following this, the draft establishes guidelines with regard to co-operation and consistency (Chapter VII). The supervisory authorities are obliged to provide each other with mutual assistance (Art 55 GDPR). The new consistency mechanism applies particularly to processing operations that may concern individuals in several Member States, but also to the determination of standard data protection clauses and the authorisation of contractual clauses and internal corporate rules. In these cases the European Data Protection Board (succeeding the Art 29 Data Protection Working Party; establishment and competences are laid out in Art 64 GDPR et seq) and the Commission may express an opinion. Moreover, the Commission is granted the power to suspend a draft measure if this is necessary to ensure the correct application of the GDPR (Art 60 GDPR) and to adopt implementing acts for the consistency mechanism (Art 62 GDPR). Both measures entail a considerable shift of power within the institutional framework of data protection laws.[27]

Remedies, liability, and sanctions are specified in Chapter VIII. The proposal provides the right to lodge a complaint with the supervisory authority (Art 73 GDPR, which also contains a right to bring representative action) as well as a new judicial remedy that can be used to require the authority to take action (Art 74 GDPR; where foreign supervisory authorities are concerned, this is complemented by the right to request the competent national authority to bring action against the foreign one). Data subjects have the right to a judicial remedy against the controller or processor either in the Member State where they are based themselves or the one where the other party has its establishment (Art 75 GDPR). Art 77 GDPR determines the right to compensation and explicitly expands this right to cover damages that were caused by the processor. Finally, Art 79 GDPR obliges the Member States to lay down rules on penalties, while Art 79 GDPR empowers the supervisory authorities for certain cases of non-compliance to impose fines up to 1 m Euro or 2 % (as opposed to 5 % in the 2011 draft) of the annual worldwide turnover.

Chapter IX contains provisions relating to specific data processing situations. This concerns the abovementioned exceptions for journalistic, artistic, and literary purposes, employment related data as well as historical, statistical, and scientific research purposes (Art 80, 82, 83 GDPR), rules on the processing of data concerning health (Art 81 GDPR), obligations of secrecy (Art 84 GDPR), and exceptions for churches and religious associations (Art 85 GDPR).

Chapter X deals in a more detailed manner with the various powers to adopt delegated acts, some of which are conferred for an indeterminate period of time while others are revocable. Additionally, the chapter contains rules on implementing acts. The final provisions of Chapter XI repeal the EDPD, explain the relation to the Directive on Privacy and Electronic Communications and establish a duty of the Commission to report on the evaluation and review of the GDPR.

4. Selected Issues of the Proposal

The proposal raises a plethora of regulatory issues which have to be discussed in the course of the legislative procedure. Out of these, four appear to be particularly worthy of discussion and further examination.

---

[27] See 4.4 below.

4.1 Scope and Transfer to Third Countries

The material scope is essentially identical to that of the EDPD. According to Recital 23, the concept of data concerning identified or identifiable persons is maintained. However, Recital 24 was turned into its opposite during the consultations: the draft had originally stated in Recital 23 that the GDPR would cover online identifiers such as IP addresses or cookie identifiers, since they can be used to create profiles of the individuals and identify them. On the contrary, the new wording suggests (logically not very convincingly) that precisely from this fact "it follows" that such data need not necessarily be considered as personal data in all circumstances.[28]

The Commission adopted the exception of personal and family-related purposes from Art 3 (2) EDPD and added for purposes of clarification that there must not be any gainful interest. In addition, the draft had stated that the GDPR was applicable nevertheless if personal data of other natural persons was made accessible to an indefinite number of individuals. Apparently, this reference to the Lindqvist case[29] was deleted at the very last moment. Nonetheless, the reasoning of the European Court in that case will apply to the new Regulation.[30]

Art 3 of the proposal contains new rules concerning the territorial scope that have evolved during the consultations. The GDPR is now applicable to controllers and processors within the Union (even if the processing takes place outside of the Union, Recital 19) and to controllers in third countries whenever personal data of individuals that reside in the Union is involved and the processing is carried out either in order to offer goods or services "in the Union" or to "monitor [the data subject's] behaviour".[31] The second alternative is described in Recital 21 as tracking individuals with data processing techniques and thus applying a profile to the individual in order to analyse or predict personal preferences, behaviours, and attitudes. This should at least apply to those social networks which, like Facebook, collect data of their customers using elements that are embedded in other websites (e.g. the "like-button"[32] and others). However, the first alternative is not explained in more detail. For instance, booking a foreign service for travels in third countries is not covered whereas ordering goods for delivery in a Member States does fall under the scope of

---

[28] Without further reasoning, the ECJ has recently described IP-addresses as personal data while neither differentiating between different groups of cases nor dealing with the discussion in scholarly literature, cf Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] C-70/10 (ECJ), para 51. The European Data Protection Supervisor ("Opinion on the Data Protection Reform Package", 7 March 2012, para 105) has strongly criticised recital 24; see also Article 29 Data Protection Working Party, "Opinion 01/2012 on the Data Protection Reform Proposals", 23 March 2012, at 9 et seq.

[29] Lindqvist v Sweden [2003] C-101/01 (ECJ), para 47; confirmed in Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy [2008] C-73/07 (COJ), para 44.

[30] See also European Data Protection Supervisor, "Opinion on the data protection reform package", 7 March 2012, para 90 et seq.

[31] Contrarily, according to the wording of the leaked draft it was decisive whether the data processing activities were "directed" to data subjects residing in the Union.

[32] See C Piltz, "Der Like-Button von Facebook" (2011) 27 *Computer und Recht* 657-664; P Voigt and S Alich, "Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber" (2011) 64 *Neue Juristische Wochenschrift* 3541-3544.

the provision. Problems may arise from the question when exactly an online-service is offered "in" the Union.

For the related issue of data transfer to third countries, Art 40 GDPR requires compliance with Chapter V and all other provisions of the GDPR. This applies to onward transfers as well. Just like the current Art 25 (4), (6) EDPD, Art 41 GDPR allows for the transfer of data based on an adequacy decision, which may now not only refer to the third country as such but also explicitly to "a territory or a processing sector" of this country or an international organisation. The criteria for the decision are specified considerably in Art 41 (2) GDPR. In case the Commission notes an inadequate level of protection, Art 41 (6) GDPR prohibits the transfer of data.

Only where the Commission has taken no decision pursuant to Art 41 GDPR, can the transfer of data be carried out based on "appropriate safeguards" in accordance with Art 42 GDPR. In particular, these can consist of binding corporate rules and standard data protection or contractual clauses that have been adopted or authorised by a supervisory authority or the Commission. The instrument of binding corporate rules is enhanced significantly in the proposal and further explained in Art 43 GDPR. It is also applicable to groups of undertakings. Corporate rules must comply with a number of substantial requirements which include, *inter alia*, a binding legal obligation, general principles of data protection, rights of the data subject, liability issues, appointment of a data protection officer, co-operation with the supervisory authority and compliance regulations. Art 43 GDPR has a very wide scope and would for example also cover cloud computing applications in corporate groups. Consequently, binding corporate rules could significantly gain practical relevance and will presumably become more important than the several individual exceptions under Art 44 GDPR.

Overall, the permissibility of data transfer to third countries is regulated in a much more detailed manner than under the EDPD. However, the issue of government access to data that has been transferred to foreign companies remains unsolved. Art 42 of the draft proposal, which was eventually deleted, would possibly have put companies in the uncomfortable situation of having to breach either foreign (particularly US) duties of disclosure or European rules on data protection.[33] In any event though, it would at least have expressed the willingness not to subordinate European protection standards to other countries' security interests. The proposal should at least have obliged controllers to inform supervisory authorities in case they are ordered to disclose data in a third country.

4.2 Rights of the Data Subject

The draft proposal changes and enhances the rights of the data subjects; moreover, Art 12 GDPR establishes procedures and mechanisms for the exercise of these rights. The rights to information and notification are specified much more concisely. The data subject's consent now needs to be "explicit" (Art 4 (8) GDPR) and express that the data subject signifies agreement with the processing of his or her data (Recital 33 emphasises the "genuine and free choice").[34] A written declaration is – contrary e.g.

---

[33] See ch 1 above.

[34] Art 4 (8) GDPR maintains that through the consent, the data subject needs to signify "agreement" to the processing. In the German translation, the wording changed from "akzeptiert" (accepts) to

to the current German requirement in § 4a (1) *Bundesdatenschutzgesetz* – not generally required. As however the controller bears the burden of proof for the data subject's consent according to Art 7 (1) GDPR, verifiable written or electronic documentation will be necessary in practice. Art 7 (3) GDPR explicitly allows the withdrawal of consent "at any time", while Art 7 (4) GDPR precludes consent, "where there is a significant imbalance between the position of the data subject and the controller". The draft had originally specified this by stating that consent shall not provide a legal basis for the processing by public authorities in the performance of their tasks or in the field of employment law. This point has now been moved to Recital 34, which has to be taken into account when interpreting Art 7 (4) GDPR. As for Germany, this would constitute a binding decision for the current debate on a federal act on data protection in the work place. The question of consent in the relationship between employer and employee has been very controversial in the parliamentary proceedings.[35]

Art 17 GDPR contains a right to erasure, which is specified and complemented by a "right to be forgotten".[36] However, the normative substance of this right can by no means live up to the aspiration promised by its strong title. Along with the familiar right to erasure, Art 17 (2) GDPR requires the controller in cases where data has been made public to "take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data". This wording is more realistic than that of the draft,[37] but technically only contains a duty to inform and not a "right". Apparently, the drafters forgot to adjust Art 17 (9) (b) GDPR, according to which the Commission shall specify conditions for the deleting duties in paragraph 2 that does not contain these duties anymore.

Another addition is the right to data portability enshrined in Art 18 GDPR. Where personal data is processed "by electronic means and in a structured and commonly used format", data subjects have the right to obtain an electronic copy of their data. The provision is presumably influenced by the discussion on social networks but goes far beyond it. The right is very important since a change of the provider is becoming increasingly burdensome if it involves the transfer of large amounts of personal data in online profiles and other databases. This bears the risk of controllers exploiting their position to the detriment of the consumer. Art 18 GDPR helps to avoid such lock-in effects. Nevertheless, the proposed provision might not completely reach its aim, as data subjects who make use of this new right will lose the possibility to keep in contact with the "friends" who stay with the former controller. This problem could only be solved by a duty to provide for interoperability.

"einverstanden" (agrees), thus indicating a slightly stronger emphasis on the free choice of the data subject.

[35] See above n 23.

[36] On this right, see B-J Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice" (2011) 8:3 *SCRIPTed* 226.

[37] The draft had contained a – hardly feasible – duty of the controller to ensure that all links and online copies were deleted.

Finally, unlike the EDPD the draft provides detailed rules on the protection of children's data.[38] According to Art 4 (18) GDPR, this includes any person below the age of 18 years. However, the most important legal consequence does not take effect up to this age limit: Art 8 (1) GDPR only requires the consent of the parent or custodian until the age of 13. Moreover, it is sufficient under Art 8 (1) 2nd sentence GDPR that, "reasonable efforts […] taking into consideration available technology" have been made in order to obtain verifiable content, thereby problematically weakening the burden of proof set forth in Art 7 (1) GDPR.

The particular need for protection of children (ie also between the age of 13 and 18) is also taken into account in several other passages of the draft, namely the provisions concerning the balancing with legitimate interests (Art 6 (1) (f) GDPR and Recital 38), the transparency requirements (Art 11 (2) GDPR: "language adapted to the data subject, in particular for any information addressed specifically to a child"; see also Recital 46), the right to be forgotten (Art 17 (1) GDPR; Recital 53 correctly emphasises the risk that children cannot fully comprehend the dangers related to data processing) and the mandatory data protection impact assessment (Art 33 (2) (d) GDPR).[39] However, a complete prohibition of measures based on profiling with regard to children was deleted from the draft. The idea is now only reflected in Recital 58.

4.3 Modern Data Protection Instruments

Recital 13 of the draft underlines the idea of technologically neutral protection, whereas Art 23 GDPR contains rules on data protection by design and default. This constitutes an urgently needed step towards connecting legal and technological protection instruments.[40] However, the draft is disappointing in this regard as it merely scratches the surface: "data protection by design" is not elaborated in any detail. Admittedly, the controller is required to implement appropriate technical and organisational measures and procedures that ensure compliance with the GDPR and safeguard the data subject's rights. Moreover, any controller must strictly adhere to the principle of necessity (Art 23 (2) GDPR). However, the draft lacks any binding statement concerning the design of the technology and does not mention general principles of data protection through technology at all (most notably, there is no mentioning whatsoever of anonymisation and pseudonymisation).[41] From a German point of view, it appears that the normative substance even falls short of § 3a *Bundesdatenschutzgesetz*, according to which "Personal data shall be collected, processed and used, and data processing systems shall be chosen and organised in

---

[38] With regard to the current legal situation, see S Jandt and A Roßnagel, "Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?" (2011) 14 *Multimedia und Recht* 637-642.

[39] See also Art 38 (1) (e) (codes of conduct), Art 52 (2) 2nd sentence (duties of the supervisory authority).

[40] See G Hornung, "Datenschutz durch Technik in Europa" (2011) 1 *Zeitschrift für Datenschutz* 51-56; on the concept see J Borking "Einsatz datenschutzfreundlicher Technologien in der Praxis" (1998) 22 *Datenschutz und Datensicherheit* 636-640; "Privacy-Enhancing Technologies (PET)" (2001) 25 *Datenschutz und Datensicherheit* 2001, 607-615; A Roßnagel (ed), *Allianz von Medienrecht und Informationstechnik* (Baden-Baden: Nomos, 2001).

[41] The Article 29 Data Protection Working Party has called for such a definition, see, "Opinion 01/2012 on the Data Protection Reform Proposals", 23 March 2012, at 11.

accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which it is collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection." Under the current draft, the practical effect of data protection by design will completely depend on the delegated acts and technical standards of the Commission pursuant to Art 23 (3) and (4) as well as Art 30 (3) GDPR. So far, the Commission has unfortunately shown little interest in legally binding obligations in this respect.

The proposal contains provisions concerning certification as well as data protection seals and marks. However, these rules are phrased even more vaguely. According to Art 39, the establishment of the respective tools are supposed to be "encouraged" by Member States and the Commission. On the contrary, the mentioned instruments – which are successfully used in the German *Land* of Schleswig-Holstein[42] – would have been deserving of binding regulations as well.[43] The draft lacks any statement as to the competent authority, the procedure, applicable criteria, and legal consequences of certification. Consequently, it is completely unclear by which standards the Commission is expected to make use of the empowerment to adopt delegated acts and lay down technical standards pursuant to Art 39 (2) and (3) GDPR.

In contrast, the provisions concerning notification of data breaches to the supervisory authority (Art 31 GDPR) and the data subject (Art 32 GDPR) are commendable. Not only do they constitute a useful instrument to ensure transparency for the data subject, they also provide controllers with an incentive to comply with legal and technical standards.[44] Moreover, the draft promotes harmonisation as it replicates in substance the corresponding provision in Art 2 (h), Art 4 (3)-(5) of the complementary Regulation 2002/58/EG.[45] It would however have been opportune to adopt the wording of the provision: there is no apparent point in using different regulatory systematics if this is not intended to imply any difference of content. The only intended difference appears to be that the supervisory ought to be notified, "where feasible", no later than 24 hours after the data breach.

---

[42] See H Bäumler "Marktwirtschaftlicher Datenschutz" (2002) 26 *Datenschutz und Datensicherheit* 325-329; H Bäumler "Ein Gütesiegel auf den Datenschutz" (2004) 28 *Datenschutz und Datensicherheit* 80-84; U Schläger "Gütesiegel nach Datenschutzaudit-Verordnung Schleswig-Holstein" (2004) 28 *Datenschutz und Datensicherheit* 459-461.

[43] On the concepts see A Roßnagel, "Datenschutz-Audit" (1997) 21 *Datenschutz und Datensicherheit* 505-515; A Roßnagel *Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung* (Wiesbaden: Vieweg, 2000); A Roßnagel "Datenschutzaudit – ein modernes Steuerungsinstrument" in L Hempel, S Krasmann and U Bröckling (eds), *Sichtbarkeitsregime, Leviathan Sonderheft* (Heidelberg: VS Verlag für Sozialwissenschaften, 2010) 263-280; H Bäumler "Audits und Gütesiegel im Datenschutz" (2001) 17 *Computer und Recht* 795-800; H Bäumler "Marktwirtschaftlicher Datenschutz" (2002) 26 *Datenschutz und Datensicherheit* 325-329; H Bäumler "Ein Gütesiegel auf den Datenschutz" (2004) 28 *Datenschutz und Datensicherheit* 80-84.

[44] On this concept, see D Gabel, "Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten" (2009) 64 *Betriebsberater* 2045-2049; J Eckhard and P Schmitz, "Informationspflicht bei Datenschutzpannen" (2010) 34 *Datenschutz und Datensicherheit* 390-397; S Ernst, "Datenverlust und die Pflicht zur Öffentlichkeit" (2010) 34 *Datenschutz und Datensicherheit* 472-475; S Hanloser, "Europäische Security Breach Notification" (2010) 13 *Multimedia und Recht* 300-303; G Hornung, "Informationen über ‚Datenpannen' – Neue Pflichten für Datenverarbeitende Unternehmen" (2010) 63 *Neue Juristische Wochenschrift* 1841-1845.

[45] The German legislator has already introduced a general regulation enshrined in § 42a BDSG.

Introducing the data protection impact assessment (DPIA) constitutes a useful measure as well.[46] It replaces the current notification requirement and is mandatory under Art 33 (1) GDPR for processing operations that "present specific risks to the rights and freedoms of data subjects". This is specified by the examples contained in Art 33 (2) GDPR, including, *inter alia*, (a) measures based on profiling (following Art 20 GDPR, although with complicated wording), (b) certain categories of data (however not adopting all categories of Art 9 (1) GDPR), (c) monitoring publicly accessible areas "on a large scale", especially when using video surveillance, (d) the processing of personal data in "large filing systems" on children, genetic data or biometric data, as well as (e) the consultation of the supervisory authority pursuant to Art 34 (2) (a) GDPR. Recitals 70 et seq contain further considerations. For instance, the subject of the impact assessment may be broader than a single project under certain circumstances (cf Recital 72).

Finally, the new right to representative action must be acknowledged. Interest groups now have the right to lodge a complaint with the supervisory authority on behalf of the data subjects concerned (Art 73 (2) GDPR) or in their own name (Art 73 (3) GDPR). On behalf of data subjects, such groups shall also have the right to engage in court proceedings pursuant to Art 76 (1) GDPR.

4.4 Institutional Aspects

Institutional and organisational provisions account for a substantial portion of the proposal. While national provisions concerning internal data protection officers (for private enterprises and public authorities) used to be optional under Art 18 (2) EDPD, some Member States such as Germany already have mandatory rules in this respect. Following a similar approach, Art 35 (1) GDPR now makes internal data protection officers mandatory for all public authorities or bodies (a) and enterprises that employ 250 persons or more (b) or engage in certain core activities (c). Pursuant to Art 35 (2) GDPR, a group of undertakings may appoint a single data protection officer in the case referred to in paragraph (1) (b), but not the case of (1) (c). In any case, data protection officers must be chosen on the basis of professional qualities and enjoy specific dismissal protection (Art 35 (5) GDPR et seq). According to Art 35 (8) GDPR, he or she may be employed by the controller or processor, or fulfil the tasks on the basis of a service contract. Art 36 and 37 GDPR determine the position and the tasks of the data protection officer.[47]

In principle, the detailed provisions should be welcomed. However, the limit of 250 employees (which corresponds with the EU definition of small and medium-sized enterprises) is not convincing. According to *eurostat*, 99.8% of all businesses within the non-financial sector of the European economy fall below this limit,[48] which makes

---

[46] With regard to technological impact assesments, see G Ropohl, *Ethik und Technikbewertung* (Frankfurt: Suhrkamp, 1996); A Grunwald, *Technikfolgenabschätzung – eine Einführung* (Berlin: edition sigma, 2010); for a general legal perspective, see A Roßnagel, *Rechtswissenschaftliche Technikfolgenforschung* (Baden-Baden: Nomos, 1993).

[47] Those tasks are in many respects reminiscent of the German *Bundesdatenschutzgesetz*.

[48] Regarding the year 2005, see M Schmiemann, "Unternehmen nach Größenklassen – Überblick über KMU in der EU" (2008) available at http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-08-031/DE/KS-SF-08-031-DE.PDF (accessed 29 Feb 2012).

this alternative negligible in practice. Also, the abstract number is not particularly helpful: it leads to the situation that Art 35 (1) (b) GDPR covers a manufacturer with 250 employees and a very small department for customer and employee data but not an address dealer whose 200 staff members exclusively engage in buying and selling personal data. In this respect, the approach taken by § 4f *Bundesdatenschutzgesetz*[49] is favourable with regard to the number of employees as well as the criterion of people dealing with automatic data processing.

Point (c) will be a key factor within the framework of Art 35 (1) GDPR as it is surely intended by the Commission to cover such cases as that of the address dealer. Unfortunately, the formulations concerning this matter differ. The introduction (p 11) and Recital 75 refer to processing operations that "require regular and systematic monitoring", whereas Art 35 (1) (c) GDPR states that such operations are relevant that "by virtue of their nature, their scope and/or their purposes require regular and systematic monitoring of data subjects". Accordingly, one refers to processing operations, the other one to data subjects being monitored. Both alternatives are possible reference points, while Recital 75 is phrased more broadly. Since special interests can be affected aside from systematic monitoring of individuals (eg by processing especially sensitive data), Art 35 (1) (c) GDPR should be altered in this respect. In any event, controllers and processors would be well advised to establish an internal compliance-management system involving a data protection officer regardless of binding obligations to do so, as the GDPR provides for extended rules concerning liability and fines.

In addition to this internal self-control, the draft mandates the establishment of supervisory authorities (Art 4 (19) and Art 46 GDPR).[50] The principle of "complete independence" that was only briefly laid down by Art 28 (1) 2nd sentence EDPD is set forth comprehensively in Art 47 GDPR, taking up the case law of the European Court.[51] Additionally, there is the duty of the Member States to provide supervisory authorities with adequate human, technical and financial resources. Art 48 GDPR lays out requirements for the appointment of the members of the authorities that can either be elected by national parliaments or assigned by governments.

The competencies and powers of the supervisory authorities have been extended compared to the EDPD. The detailed regulation of Art 52 GDPR covers several duties that concern monitoring, complaints, information, investigation, consultation, authorisation, and participation. The powers established by Art 53 GDPR are phrased precisely and include a variety of measures to exert influence on data processing as well as the right to obtain access to controllers' premises, which is to be regulated by Union or Member State law. Controllers are obligated to co-operate with the supervisory authorities under Art 29 GDPR. Art 79 GDPR provides a gradual system of administrative sanctions. The fines can amount up to 1 m Euro or 2% of the worldwide annual turnover but need to be "in each individual case effective, proportionate and dissuasive". The respective provisions cover a wide range of breaches of the GDPR.

---

[49] See 2 above.

[50] The German approach of establishing several authorities is explicitly permitted. However, one of them shall be designated as a "single contact point" pursuant to Art 46 (2).

[51] *European Commission v Federal Republic of Germany* [2010] C-518/07 (ECJ).

Art 74 GDPR regulates the right to a judicial remedy against a supervisory authority no matter whether the individual seeks remedy against a decision or seeks to oblige the supervisory authority to act on a complaint. Contrary to the draft, an individual may not bring proceedings in his or her own country of residence if a foreign supervisory authority is concerned. Apart from bringing proceedings in the other Member State itself, the data subject may now alternatively "request" the supervisory authority of the Member State where it has its habitual residence to do so on its behalf.

Art 51 GDOR significantly changes the competence rules. While each supervisory authority normally covers the territory of the respective Member State, special rules apply to enterprises that are established in more than one Member State. In this case, Art 51 (2) GDPR states that the supervisory authority of the main establishment (cf Art 4 (13) GDPR) shall be exclusively competent for the entire enterprise. Presumably, this will cause conflicts with supervisory authorities and courts of other Member States. Pursuant to Art 75 (2) 2nd sentence GDPR, it is possible to bring proceedings against controllers based in other Member States before courts in the country of habitual residence. This results in the possibility of a competent supervisory authority approving a processing operation, while the same operation is dismissed by the court of a different Member State.

Concerning the relationship between the different supervisory authorities in trans-border cases, Art 56 GDPR requires joint operations which include authorities of all Member States where individuals are likely to be affected. Their members of staff may carry out investigative tasks while the host authority assumes responsibility for their actions.

From the controllers' and processors' point of view, it would certainly constitute a great simplification if all competences were concentrated with one central supervisory authority. This can however only be justified if the Member States not only have highly consistent standards, but also the respective supervisory authorities apply them uniformly. At the moment, the common practice falls short of this goal because the authorities interpret their role very differently under the current guidelines set forth by the EDPD. There is thus the risk of a race to the bottom if enterprises, when choosing a place for their main establishment could "pick" a supervisory authority that interprets the GDPR in their favour.

In certain cases, the draft requires the so-called "consistency mechanism" (Art 57 GDPR et seq) in addition to the supervisory authorities' general duty to co-operate with each other and the Commission (Art 46 (1) 3rd sentence GDPR). With the exception of some resemblance to Art 26 (3) EDPD, this is a novelty. The mechanism applies to a variety of cases: Art 58 (2) GDPR mentions processing activities concerning the offering of goods or services to data subjects in several Member States or the monitoring of their behaviour, substantial impairment of the free movement of personal data, determining standard data protection clauses, authorisation of contractual clauses and approval of binding corporate rules.

Presumably, the mechanism will be applied to a vast number of cases, especially due to the first two alternatives. It is initiated when requested by a supervisory authority, the European Data Protection Board or the Commission. The latter two may issue opinions pursuant to Art 58 (7), 59 GDPR. The competent supervisory authority shall take "account" of the Board's opinion and the "utmost [ie stronger] account" of the opinion issued by the Commission under Art 59 (2) GDPR. There is also a duty on the

supervisory authority to inform the Commission and the Board about its intentions to amend measures. After this point, the European Data Protection Board is not involved anymore. If however the Commission disagrees with the result, it may adopt a reasoned decision under Art 60 GDPR requiring the supervisory authority to suspend the measure for a maximum of twelve months (the German version of the Commission's draft reads: "twelve weeks") in order to adopt a measure pursuant to point (a) of Art 62 (1) GDPR. This provision authorises implementing acts for the "correct application" of the GDPR, which consequently is decided on by the Commission within the framework of the consistency mechanism.

5. Preliminary Conclusions

The Commission has taken on the Herculean task of fundamentally reforming the European data protection law. This alone must be recognised, bearing in mind that for example the German legislator has been reluctant to initiate fundamental reforms in this area for years. The tremendously expanded amount of regulations in the draft illustrates – since no regulatory matter appears to be unnecessary – the increased complexity of data protection in modern information societies.

Concerning the content, the draft offers both light and shade. Substantial new rules concerning data subjects' rights, technological and organisational duties, competences of supervisory authorities, the role of data processors, and sanctions are commendable. Other points (especially the modern protection instruments) constitute decent ground rules that should be extended in the course of further legislative procedure.

However, the eminently strong position of the Commission is not justified.[52] The proposal entails a serious institutional shift in this respect, as the Commission currently only assumes decision-making competence in selected areas[53] but is now intended to become active in all important regulatory sectors. A large number of Articles contain competences to adopt delegated acts (Art 86 GDPR, cf Art 290 TFEU) and/or implementing acts (Art 87 (2) and (3) GDPR, cf Art 291 TFEU). In light of the rapid technological progress, these instruments may constitute a useful approach in order to react with flexible and fast regulatory measures.[54] It will also be advisable in many cases to create uniform requirements and guidelines for practice. However, the draft provides so many authorisations on substantial parts of the proposal (note the extensive catalogue of Art 86 GDPR), that the overall picture hardly complies with Art 290 (1) TFEU that authorises delegated acts only if they

---

[52] See also European Data Protection Supervisor, "Opinion on the Data Protection Reform Package", 7 March 2012, para 71 et seq.; Article 29 Data Protection Working Party, "Opinion 01/2012 on the data protection reform proposals", 23 March 2012, at 6 and 20.

[53] Cf Art 25 (4) and (6), Art 31 (2) EDPD regarding the power to issue adequacy decisions and Art 26 (4) regarding the recognition of standard contractual clauses.

[54] Cf European Data Protection Supervisor, "Opinion on the Communication from the Commission" (2011) available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf (accessed 29 Feb 2012) 24; A Roßnagel, "Nicht mehr zeitgemäß. Das Datenschutzrecht ist unübersichtlich und widersprüchlich. Der traditionelle Schutz informationeller Selbstbestimmung steht in Frage" (2011) 1 Jun *Frankfurter Allgemeine Zeitung* 7; G Hornung, "Datenschutz durch Technik in Europa" (2011) 1 *Zeitschrift für Datenschutz* 51-56 at 56.

supplement or amend certain "non-essential elements" of the legislated act.[55] This is of special concern in areas such as data protection by design and by default (Art 23 GDPR) or certification (Art 39 GDPR),[56] where the GDPR is limited to naming basic principles and leaves it up the Commission to decide all significant legal questions. These and other provisions cannot even be applied in practice until the corresponding delegated acts are adopted. Finally, it is simply unacceptable to exclude an entire regulatory area such as processing in the employment context and subject it to the legislation of the Member States (Art 82 (1) GDPR)[57] and still empower the Commission to adopt delegated acts in this area (Art 83 (3) GDPR).

The Commission's decision-making competence within the consistency mechanism clearly contravenes the position of the national supervisory authorities. The draft forces Member States to grant the latter complete independence. On a European level however, an institution would have the final say whose composition, organisation and working methods by no means reflect the principles of independent data protection supervision.[58]

Taken as a whole, the Commission would gain a range of competences that is inadequately wide, raises concerns with regard to primary law and is contrary to the system of supervisory authorities. Consequently, several passages of the draft should set forth more specific requirements for delegated acts, while the role of the Commission should be restricted to the development of generally applicable guidelines. Where specific Europe-wide decisions are necessary, the future regulation should provide for an independent, well-appointed European institution (for instance a European Data Protection Board with extended competences) that is subject to judicial review just like the national supervisory authorities. Dividing the tasks in such a way would increase the chance that the proposed substantive rules are put into practice effectively.

---

[55] See also European Data Protection Supervisor, "Opinion on the Data Protection Reform Package", 7 March 2012, para 74; Article 29 Data Protection Working Party, "Opinion 01/2012 on the Data Protection Reform Proposals", 23 March 2012, at 7. The conflict with Art. 290 (1) TFEU applies even keeping in mind that the ECJ has granted a significant leeway as regards this requirement (see K Gärditz, "Die Verwaltungsdimension des Lissabon-Vertrags" (2010) 63 *Die Öffentliche Verwaltung* 453-465; C Möllers and J von Achenbach, „Die Mitwirkung des Europäischen Parlaments an der abgeleiteten Rechtsetzung der Europäischen Kommission nach dem Lissabonner Vertrag" (2011) 46 *Europarecht* 39-61). The ECJ eg decided that "such classification [ie as essential] must be reserved for provisions which are intended to give concrete shape to the fundamental guidelines of Community policy, cf Federal Republic of Germany v European Commission [1992] C-240/90 (ECJ), para 37.

[56] See 4.3 above.

[57] The Commission's approach to establish a European regulation for this area was not pursued any further after the year 2001.

[58] See also European Data Protection Supervisor, "Opinion on the Data Protection Reform Package", 7 March 2012, para 242 and 248 et seq.