Data protection for the digital age: comprehensive effects of the evolving law of accountability

Senior assistant – lecturer Ph.D. **Nina GUMZEJ**[1]

Abstract

The law of personal data protection has for years been lagging behind technology, which is evolving propulsively and with high speed. A number of new challenges arising from the post-modern digital age have been identified for rights and freedoms of individuals with respect to processing of their personal data and thus a need for adapting the relevant legal-regulatory regime and ensuring a workable and systematic data protection system for the third millennium. After examination of the current legal framework and supporting systems at the level of European Union law, this paper focuses on recently proposed reforms. Proposed new EU legal-regulatory regime towards a potent data protection ecosystem is strongly supported by stricter accountability of those who are responsible for personal data. As one of the core legal principles supporting the new regime, accountability denotes, in a nutshell, a number of legally enforceable duties to implement and verify measures and procedures that can ensure operative and demonstrable data protection compliance. Selected highlights of the proposed accountability measures are therefore examined in this paper and arguments provided for a shift towards organizational data protection management and governance already today.

Keywords: *right to personal data protection, accountability, compliance, data controller, digital age, Proposal for a EU General Data Protection Regulation*

JEL Classification: K20

Introduction

The need and means to ensure special protection of human rights with respect to processing of personal data pertain to the development of informatics technology in the course of the 1960s. A transition towards automated processing of information with the assistance of computers enabled a significant increase in speed, reliability and capacity of processing and storage of information, and with the development of computer networks provided for their exchange and unhindered transmission. In such circumstances, especially taking into account the social context of initiated globalization and the need to ensure free flows of information, special protection of personal data started to become recognized as a prerequisite for continued unconstrained enjoyment of guaranteed human rights and freedoms in the area of information and communications privacy. At the same time this resulted from societal reactions to the growing abuse starting to take place with respect to personal data stored in digital databases in the public sector and followed by the private sector. In these circumstances, attempts to eliminate risks or at least bring them under control followed with the

[1] Nina Gumzej, Faculty of Law, University of Zagreb, Croatia, nina.gumzej@pravo.hr

establishment and enforcement of special rules, which established *inter alia* the conditions for collection, processing and use of personal data as well as sanctions in cases of abuse. These rules also introduced a number of obligations for those who collect and further process personal data and at the same time prescribed rights in relation to this for relevant individuals, *i.e.*, data subjects.

With the ensuing development towards the global information society electronic communications became essential, and ever more so in light of evolution of digital networks and a myriad of innovative new services to be provided with the use of information-communication systems. Together with the digitalization of networks and services and the availability of computers and other terminal equipment, modern technology has targeted evolution towards ultra-speed networks and the growingly advanced convergence of different electronic communications devices and services, intended for widespread use. In the post-modern digital age individuals are growingly communicating online and carrying out their day-to-day activities online and it could be said that networked presence is becoming vital for their ability to satisfy various needs, whether for purely personal, social and entertainment purposes, or for business purposes. Digital uptake trends are complemented by increasingly free or at least economically viable solutions offering virtual data storage and other online data processing services, such as cloud computing. At the same time, intensified and more complex forms of processing personal data online further accentuate the problem of managing control over them in borderless cyberspace. Furthermore, with the aid of technology digital presence of individuals and their activities and dispositions are not difficult to trace, and processing massive sets of data relating to them is enabled in a growingly sophisticated manner. In addition to this emphasis in the highly competitive market economy is increasingly placed on tailor-made services and products, *i.e.*, personalization on the basis of individual preferences, which is enabled by tracking and profiling of networked individuals, so as to target their anticipated needs, habits and interests as accurately as possible. Indeed, personal data have, as it is often said become a new commodity, supported by evolving markets for such data, but at the same time it has become clear that the digital economy depends also on confidence of the consumers that their data will be processed lawsfully, and securely. Inevitably, the globally networked communications environment produces significant risks for the security of information systems and for personal data, with acts of cybercrime amassing and further evolving along with the overall trend towards the digital life. What cannot also be ignored is intensified surveillance over individuals on account of the need to effectively fight serious criminal acts such as terrorism, which also implies increased and more sophisticated monitoring of personal data, as well as use thereof, including the data originally collected from the individual to be used only for commercial purposes.

All the aforementioned issues bring to light the more progressive challenges in the post-modern digital age for rights and freedoms of individuals with respect to

processing of their personal data, while highlighting the requirement to provide for their more effective assurance and enforcement.

Harmonization of national legal frameworks in the general area of personal data protection was at the EU level initiated with the *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*[2]. Later on, the right to personal data protection itself has at the level of EU law evolved to a fundamental human right. Currently a legislative process is ongoing towards a thorough reform of the EU data protection regime, and the aim in respect of individuals' rights is providing for more efficient protection thereof, especially in light of the advanced challenges of the digital age. A proposed prerequisite for this reform lays in the empowered regulatory platform towards a *truly workable* ecosystem that provides for demonstrable data protection compliance by the responsible persons or entities.

This paper focuses on the stated aim, and more specifically on aspects of the legally enforceable and reinforced accountability in data protection that transpose the regulatory data protection paradigm towards the uptake of appropriate organizational, management and governance models so as to ensure systematic compliance in this area. Following an introductory overview of the general personal data protection legal-regulatory regime with an emphasis on harmonization mechanisms under EU law in section 2 I will examine the more recent important developments in this area at the EU law level, and provide introductory explanations on reinforced accountability in the proposed new EU (general) data protection rules as well as a basic overview of evolving frameworks towards enforceable accountability in data protection. In the next section I will analyze selected aspects of proposed new EU data protection legal-regulatory framework, while also reflecting on findings from the preceding analyses. This is followed by a more in-depth analysis of selected key accountability elements of proposed EU rules in section 4. In the conclusion I will reflect on results of my research and argument my proposal for early implementation of certain preliminary accountability mechanisms in relevant organizations.

1. The current regime and need for reform

In this paper I will focus on Directive 95/46/EC as the main EU legal instrument regulating personal data protection at a general level[3], and especially

[2] 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, Official Journal of the European Union L 281, 23.11.1995, pp. 31-50.

[3] See Art 3. and recital 27. of Directive 95/46/EC. I will exclude from this analysis the more specific area of data protection, such as the police and judicial cooperation in the context of law enforcement. For more details on personal data protection rules in this area, see the 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, Official Journal of the European Union L 350, 30.12.2008., pp. 60-71., as well as the European Commission's

on the proposed revision of this directive by the European Commission from January 2012[4]. Though not examined in this paper it is nonetheless appropriate to make a reference here to the special data and privacy protection rules for the electronic communications sector (*Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications*[5]), in light of the challenges for data protection arising in this area, and the globally networked surroundings in general.

Adoption of Directive 95/46/EC was apart from the need to ensure harmonized levels of protection of rights, and especially privacy rights, of individuals with respect to processing of their personal data in Member States also triggered by economic interest, *i.e.*, removal of barriers to unhindered functioning of the internal market and hence to the free flow of personal data[6]. Uniformity in application of the directive is ensured by legally binding interpretations provided by the Court of Justice of the European Union, normally in a preliminary reference procedure, when and if initiated in the relevant area. Important role towards harmonization of national rules adopted on the basis of Directive 95/46/EC and co-operation with national data protection supervisory bodies was assigned by this directive itself, to the independent advisory body for the protection of personal data and privacy - *The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data* („Working Party")[7]. Namely, the Working Party is *inter alia* authorized[8] to examine any question with respect to the application of national measures adopted under the Directive 95/46/EC so as to contribute to their uniform application, as well as make recommendations (on its own initiative) on all

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, 2012/0010 (COD), Brussels, 25.1.2012.

[4] European Commission, *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, 2012/0011 (COD), Brussels, 25.1.2012.

[5] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Union L 201, 31.7.2002, pp. 37-47. This Directive was last revised in 2009: Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Official Journal of the European Union L 337, 18.12.2009, pp. 11-36.

[6] In this sense see Art. 1. as well as recitals 1-11. of Directive 95/46/EC.

[7] Working Party is composed of representatives of supervisory data protection authorities of each EU Member State, the European Data Protection Supervisor as representative of EU institutions and bodies, and a representative of the European Commission. For more details see Art 29., as well as recital 65. of Directive 95/46/EC.

[8] Art. 30. of Directive 95/46/EC.

matters relating to protection of persons with regard to processing of personal data in the EU. It also informs the European Commission if it finds divergences in the laws or practices of Member States that are likely to affect equivalence of protection of individuals in relation to personal data processing in the EU. Working Party is authorized not only to advise the Commission on the proposals to amend the Directive 95/46/EC, but also on any additional or specific measures to safeguard rights and freedoms of individuals in relation to personal data processing, and on any other proposed EU measures influencing those rights and freedoms. After having been called by the Commission the Working Party also carries out the objective of ensuring better harmonization of national rules implemented on the basis of Directive 95/46/EC by way of the so-called „joint enforcement actions" throughout different industries, in co-operation with the national data protection supervisory authorities[9]. It also issues recommendations, opinions and working documents, as well as annual reports, which are publicly available[10]. Its opinions and recommendations are delivered to the European Commission and the committee assisting it[11], and the Commission is obliged to notify the Working Party on action taken as to these. Over the course of years the Working Party adopted a large number of opinions, recommendations and working documents on various data protection issues intending to contribute to better harmonization in application of the directive. While fact is that adopted common positions of the Working Party are not legally binding, there are views that such positions should be considered authoritative[12]. In the impact assessment accompanying its proposal for the new general EU data protection rules

[9] Such actions were carried out in the medical insurance sector, see: Article 29 Data Protection Working Party, *Report 1/2007 on the first joint enforcement action: evaluation and future steps*, 01269/07/EN, WP 137, 20.6. 2007; and the electronic communications sector - Note: tasks of the Working Party also extend to the relevant area in the electronic communications sector, see Art. 15. Para. 3. (and recital 48) of Directive 2002/58/EC in connection with Art. 30. of Directive 95/46/EC. See: Article 29 Data Protection Working Party, *Joint Investigation Action on the Implementation of the Data Retention Directive*, Press Release, 10.12.2008., available at: http://ec.europa.eu/justice/policies/privacy/news/docs/pr_17_03_09_en.pdf (last accessed 27.9.2012.); Article 29 Data Protection Working Party, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*, 00058/10/EN, WP 172, 13.7. 2010. It should be noted here that despite the fact that the opinions and recommendations the Working Party adopts are not legally binding, when establishing data protection compliance in the sector the Working Party does check if its recommendations on a relevant subject-matter are observed by the Member States, see *ibid.*

[10] These are available *online* at: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm (last accessed 27.9.2012).

[11] Art. 31. of Directive 95/46/EC.

[12] See, e.g.: European Network and Information Security Agency, *The Article 29 Working Party recommendations, consultations and policy documents*, available at: http://www.enisa.europa.eu/act/rm/cr/laws-regulation/data-protection-privacy/article-29-working-party ((last accessed 27.9.2012); Christopher Kuner, *European data protection law - Corporate compliance and regulation*, Oxford University Press, New York, 2nd ed., 2007, p. 10. (point 1.19).

(regulation), the European Commission noted that while in certain cases Working Party's opinion did have some impact on national legislation and practice, these are not always followed by the national data protection authorities[13].

The European Data Protection Supervisor („EDPS"), independent supervisory authority in charge of ensuring respect for the right to personal data protection and privacy in the institutions and bodies of the EU[14] is the other very important advisory body to the Commission[15] in the overall EU data protection framework. The EDPS, namely, advises (on its own initiative or in response to a consultation) EU institutions and bodies as well as data subjects on all matters concerning personal data processing[16]. Importance of its role is also signified by the Commission's duty to consult the EDPS when adopting legislative proposals concerning the protection of rights and freedoms in relation to personal data processing[17]. Opinions of the EDPS are official and publicly available[18], as well as other relevant documents, such as comments[19].

Entering of the Lisbon Treaty[20] into force in 2009 and abolishment of the pillar-structure of the European Union provided for legal prerequisites for a reform in the approach toward regulating personal data protection at the level of EU law. Today the right to personal data protection is guaranteed to everyone pursuant to Article 16. of the Treaty on the Functioning of the European Union (TFEU)[21]. This Article also establishes that the European Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices

---

[13] European Commission, *Commission Staff Working Paper, Impact Assessment - Accompanying the document 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) and 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*, SEC(2012) 72 final, Brussels, 25.1.2012, p. 18.; also see Annex 2 to the Impact Assessment: Evaluation of the implementation of the Data Protection Directive, section 10.13.

[14] See: 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, Official Journal of the European Union L 8, 12.1.2001, pp. 1-22.

[15] For details on EDPS consultations, see: http://www.edps.europa.eu/EDPSWEB/edps/Consultation (last accessed 27.9.2012).

[16] See Art. 41. Para. 2., as well as Art. 46 d of Regulation no. 45/2001.

[17] Art. 28. para. 2. of Regulation no. 45/2001.

[18] See: http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation/OpinionsC (last accessed 27.9.2012).

[19] See: http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Comments (last accessed 27.9.2012).

[20] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, Official Journal of the European Union C 306, 17.12.2007, pp. 1-271.

[21] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Official Journal of the European Union C 83, 30.3.2010, p. 47.

and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data, in the ordinary legislative procedure[22]. Moreover, compliance with these rules is to be subject to control of independent authorities. It is also important to point to the Charter of Fundamental Rights of the European Union[23]. Namely, in Article 8 of the Charter the right to personal data protection is established as a separate fundamental right[24].

After having launched public consultations on the legal framework for th new fundamental right to personal data protection right in 2009[25], the Commission released in 2010 a Communication[26] containing its strategy towards modernizing the current legal framework (Directive 95/46/EC). As previously explained, reform of the relevant legal-regulatory regime was considered necessary especially in light of new challenges to the right to personal data protection as brought by the rapidly evolving technological developments and globalization. A review of certain solutions of the current regime also called for better adaptation of the relevant legal framework for the internal market structure, especially taking into account the administrative and financial burdens, which the organizations handling personal data with relevant business operations in several Member States were facing. This Communication was also followed

[22] For stipulated derogations in specific areas such as in particular the area of common foreign and security policy, see Article 39. of the Treaty on European Union in connection with Article 16. para. 2. (last sentence) of the Treaty on the Functioning of the EU. Also see a *Declaration on Article 16 of the Treaty on the Functioning of the European Union*, Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007, Official Journal of the European Union C 83, 30.3.2010, p. 345.

[23] Charter of Fundamental Rights of the European Union, Official Journal of the European Union C 83, 30.3.2010, pp. 389-403. The Charter has same legal force as the Treaties (Art. 6. para. 1. of the Treaty on European Union). It obliges institutions, bodies, offices and agencies of the EU, as well as Member States when they are implementing EU law (for more details see Art. 51. of the Charter).

[24] It is separate from the right to respect of private life in Art. 7. of the Charter. The Court of Justice of the European Union established a close connection between the fundamental right to personal data protection in Art.8. of the Charter, and the right to respect of private life in Art. 7. This right to respect for private life with regard to personal data processing as recognized in Arts. 7. and 8. of the Charter concerns any information relating to identified or identifiable individual. The Court also established that the right to personal data protection is not absolute, but needs to be considered with respect to its function in society. Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, 09.11.2010, Court of Justice of the European Union, European Court reports 2010, p. I-11063, see especially paras. 47-52. To be noted here is also that Art. 7. of the Charter corresponds to Art. 8. of the Council of Europe Convention for the protection of human rights and fundamental freedoms, CETS No. 005, 4.11.1950. While the right to personal data protection is not recognized in text of this Convention, the European Court of Human Rights has interpreted aspects thereof in light of the mentioned Art. 8. of the Convention.

[25] Available at: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm (last accessed 27.9.2012).

[26] European Commission, *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, Brussels, 4.11.2010.

by public consultations during 2010-2011[27]. Following analysis of contributions received in public consultations and a comprehensive impact assessment, the Commission issued a Proposal for General Data Protection Regulation[28] (further also as: "Proposal" or "Proposal for Regulation") in January 2012, noting that it is "time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities"[29]. Unlike Directive 95/46/EC[30], the Commission's Proposal mostly focuses on the (newly) established fundamental right to personal data protection as explained above, laying down rules relating to protection of individuals with regard to personal data processing (and rules relating to free movement of data), with an objective of protecting their fundamental rights and freedoms and in particular their right to personal data protection[31]. The proposed new rules intend to reinforce relevant rights of data subjects[32], also by introducing certain new rights such as the right to data portability[33] and better adapt enforcement of these rights in the overall context of the largely technology-driven, post-modern digital age. At the same time they addresses concerns of organizations in charge of processing data with respect to certain data protection mechanisms that impose significant administrative as well as financial burdens on them and their business operations, most notably in cases of processing operations taking place in several Member States (such as the requirements on notifications of data processing operations and requirements on international data transfers). Many problems in this sense have resulted from differences in implementation of Directive 95/46/EC in Member States' national laws[34]. Diversity in nationally implemented

---

[27] Available at: http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm (last accessed 27.9.2012).

[28] European Commission, *op. cit*. at note 3.

[29] European Commission, *op. cit*. at note 3, p. 2.

[30] Art. 1. para. 1. of Directive 95/46/EC.

[31] See Art. 1. paras. 1-2. as well as recitals 1-2. of the Proposal. For a general critique on the approach used in the proposed Regulation vis-à-vis such disconnection of privacy from data protection, see Luiz Costa, Yves Poullet, *Privacy and the regulation of 2012*, „Computer Law & Security Review", Elsevier, Vol. 28, Issue 3, 2012, pp. 254-262 at p. 255 (section 3).

[32] Some of the relevant provisions in the Proposal are, for example: Article 11 - transparent information and communication; Article 12 - procedures and mechanisms for exercising the rights of the data subjects; Art. 14. - information to the data subject; Art. 17. - right to be forgotten and right to erasure; Art. 19 - right to object.

[33] Proposed right to data portability would enable data subjects to get a copy of their data from the controller, and also to transfer data (for example, to another service provider), all in a commonly used electronic format. See Art. 18. of Proposal for more details.

[34] For analyses on implementation of Directive 95/46/EC in Member States, see the following studies for the Commission: Douwe Korff, *EC study on implementation of data protection directive - Study Contract ETD/2001/B5-3001/A/49, Comparative summary of national laws*, Colchester – Cambridge: University of Essex, 2002., available at: http:// ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf (last accessed 27.9. 2012); Douwe Korff, *Comparative study on*

solutions could not be overcome effectively – also despite the previously explained work towards harmonization and tasks entrusted to that effect to special bodies, such as the Working Party[35]. In addition to the fact that directive itself leaves a margin for *manoeuvre* for implementation in national law[36], it is by legal nature only binding on Member States as to the result that must be achieved, but national authorities have the choice on the form and methods[37]. Conversely, a regulation is entirely binding and directly applicable in all Member States, and it has general application[38]. This is, therefore, proposed legal instrument to ensure uniformity, which is considered necessary in the area of general personal data protection examined in this paper.

The Proposal has been referred to the European Parliament and the Council (ordinary legislative procedure). While I will not especially point to this issue throughout all the new provisions examined in this paper, it is appropriate to here bring notice to the by now already widely criticized new powers envisaged for the European Commission, which would be authorized to adopt non-legislative delegated and implementing acts over a large number of areas covered in the Proposal. This adds up to the debate on required clarity of the new rules, and the overall legal certainty in the area. It has been reported that adoption of final text of the new rules is hopefully expected to take place already during Ireland's Presidency of the Council in 2013[39]. Political pressure to have the new rules adopted fast and numerous criticisms of the Proposal already expressed in particular by the Member States are likely to lead to an agreement over a significantly revised text, including on previously stated grounds. As to the time frame for applicability of the new rules, according to the transition period set in Article 91 of the Proposal, the new rules, *i.e.*, Regulation is to apply in Member States two years from its entering into force.

---

different approaches to new privacy challenges, in particular in the light of technological developments - Contract No. JLS/2008/C4/011 – 30-CE-0219363/00-28, Working paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments, LRDP KANTOR Ltd (Leader) - Centre for Public Reform 20.1.2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf (last accessed 27.9.2012).

[35] European Commission, *op. cit*. at note 12.

[36] See recital 9. of Directive 95/46/EC and as an example of such provision see Art. 8. paras. 4-5 of Directive 95/46/EC.

[37] Art. 288. para. 3. of the Treaty on the Functioning of the European Union.

[38] Art. 288. para. 2. of the Treaty on the Functioning of the European Union.

[39] Maria Koleva, *Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner: We need our citizens on board*, Brussels, „Europost", 07.9.2012, available online at: http://www.europost.bg/article?id=5331 (accessed 27.9.2012). Also see the calendar set for Data Protection Regulation (European Parliament), which is available online at: http:// www.europarl. europa.eu/document/activities/cont/201209/20120926ATT52342/20120926ATT52342EN.pdf.

2. Frameworks for enforceable accountability in data protection

Calls for reinforced accountability in the new EU data protection legal-regulatory framework can be summed up in the following statement of the Working Party: „*Data protection must move from 'theory to practice'. Legal requirements must be translated into real data protection measures*"[40]. Next to Working Party's efforts towards promoting reinforced accountability in the new rules[41] (and also called for by the European Data Protection Supervisor[42]), the Commission embraced the core elements of the concept in its Proposal, following analysis of all contributions in public consultations and an impact assessment. This resulted in the proposed general duty of data controllers as responsible persons/entities for personal data processing, to implement policies and measures to ensure processing of data in compliance with data protection rules, demonstrate such compliance to data protection supervisory authorities, as well as to adopt mechanisms to verify the efficiency of implemented measures[43]. Relevant measures would *inter alia* include a duty to keep documentation on personal data processing, enforce security measures, carry out data protection impact assessments in certain special cases where processing would entail specific risks to rights and freedoms of individuals, as well as consult with the data protection supervisory authority prior to certain risky processing operations, appoint the data protection officer, and a duty to administer mechanisms for controlling efficiency of implemented measures, *e.g*. via audits. In section 4 I will provide a more in-depth analysis of selected key measures reflecting enforceable accountability requirements in the Proposal.

A framework towards enforceable accountability in data protection is also evident in relevant activities of the Council of Europe and it is here important to point to the more recent key developments on the *Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data*[44]. This Convention has to date remained the only internationally legally binding instrument in personal data protection, to which also states that are not Members States of the Council of Europe can accede[45]. The Convention is

---

[40] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, 00062/10/EN, WP 173, 13.7. 2010. p. 1.

[41] Article 29 Data Protection Working Party and 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*, 02356/09/EN, WP 168, 1.12.2009; Article 29 Data Protection Working Party, *ibid.*

[42] See, e.g.: *Opinion of the European Data Protection Supervisor 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*', Official Journal of the European Union C 181, 22.6.2011, pp. 1-23. at section 7.2.

[43] In this respect see in particular Article 22. and recital 60. of the Proposal.

[44] Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 28.1.1981.

[45] For calls to have as many states acceding to it, globally, see, e.g.: *The Madrid Privacy Declaration - Global Privacy Standards for a Global World*, 3.11.2009, 31st annual meeting of the International Conference of Privacy and Data Protection Commissioners, Madrid, 4-6.11.2009, available at: http://thepublicvoice.org/madrid-declaration/ (last accessed 27.9.2012).

currently in review[46], and, also in parallel with the relevant developments at EU law level, principle of accountability as one of the key elements has been introduced in the revision. Main proposed duty of the contracting parties to the Convention is to provide that the responsible persons or entities (the controller, *or where applicable the processor*) take at all stages of data processing all appropriate measures to implement the provisions giving effect to principles and obligations of the Convention, and establish internal mechanisms to verify and demonstrate compliance of data processing under their responsibility to both the data subjects and data protection authorities[47].

In examination of origins of accountability in data protection it should be acknowledged that this is neither an entirely novel data protection principle, as the principle was first recognized already in the *Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* from 1980[48], nor is it a principle exclusively deriving from the European legal tradition, since it is one of the information privacy principles in the 2004 Asia-Pacific Economic Cooperation (APEC) Privacy

[46] For more details on the ongoing review, *i.e.*, modernization of the Convention, see: http:// www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp (last accessed 27.9.2012).

[47] „(1) Each Party shall provide that the controller, or where applicable the processor, shall take at all stages of the processing all appropriate measures to implement the provisions giving effect to the principles and obligations of this Convention and to establish internal mechanisms to verify and demonstrate to the data subjects and to the supervisory authorities provided for in Article 12 bis of this Convention the compliance of the data processing for which he/she is responsible with the applicable law. (2) Each party shall provide that the controller shall carry out a risk analysis of the potential impact of the intended data processing on the rights and fundamental freedoms of the data subject and design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights. (3) Each Party shall provide that the products and services intended for the data processing shall take into account the implications of the right to the protection of personal data from the stage of their design and facilitate the compliance of the processing with the applicable law. (4) The obligations included in the domestic law on the basis of the provisions of the previous paragraphs may be adapted according to the size of the processing entities, the volume of data processed and the risks for the interests, rights and fundamental freedoms of the data subjects." Article 8 bis – Additional obligations. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Final document on the modernisation of Convention 108*, T-PD(2012)04 rev en, Strasbourg, 17.9.2012, available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04_rev_en.pdf (last accessed 27.9.2012). Also see draft elements for the Explanatory Report (currently available only with respect to earlier version of proposed Article 8 bis): Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Final document on the modernisation of Convention 108*, T-PD (2012)04Mos, Strasbourg, 15.6.2012, p. 39 (paragraphs 67-72), available at: http:// www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04Mos.pdf (last accessed 27.9.2012).

[48] Paragraph 14. of the OECD Guidelines (accountability principle). For detailed comments, see paragraph 62. of the Explanatory Memorandum to the Guidelines. Text of the OECD Guidelines and the Explanatory Memorandum is available at: http:// www.oecd.org/ document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html (last accessed 27.9.2012).

Framework[49]. It is also a statutory requirement in certain countries, such as Canada (*Personal Information Protection and Electronic Documents Act -"PIPEDA"* from 2000)[50]. As regards the official practical advice on implementation of stated statutory requirements, I would point to the recently issued guidelines by the Canadian privacy commissioners, with concrete steps towards implementation of accountability requirements in organizations by way of appropriate privacy management programs[51].

More detailed information on considerations towards implementing accountability requirements in organizations, such as via appropriate privacy programs, as well as on the development of frameworks for enforceable data protection accountability can be found by consulting the relevant activities of the Centre for Information Policy Leadership ("Accountability Project")[52].

3. Selected aspects of the future data protection regime

It would seem safe to conclude, in terms of broad concepts of a data subject and personal data relating to him or her (including the acknowledgment of digital identifiers or online identifiability), that unless responsible (persons or) entities processing personal data employ appropriate techniques to render such data truly anonymous (and, of course, when and if such processing makes

---

[49] See principle IX (point 26) of the APEC Privacy Framework, December 2005, APEC Secretariat, Singapore, available at: http://publications.apec.org/publication-detail.php?pub_id=390 (accessed September 27, 2012). For details on APEC work on cross-border privacy rules towards accountability in cross-border data flows, see point 48 of the APEC Privacy Framework and details on the „APEC Data Privacy Pathfinder" (2007): APEC, *APEC Data Privacy Pathfinder Projects Implementation Work Plan – Revised, submitted by Australia*, 2009/SOM1/ECSG/SEM/027, First Technical Assistance Seminar on the Implementation of the APEC Data Privacy Pathfinder, Singapore, 22-23 February 2009, available at: http:// aimp.apec.org/Documents/2009/ ECSG/SEM1/09_ecsg_sem1_027.doc (last accessed 27.9. 2012).

[50] Schedule 1 (point 4.1: Principle I – Accountability) of the Personal Information Protection and Electronic Documents Act, SC 2000, c 5, available at: http://canlii.ca/t/l29k (last accessed 27.9.2012)

[51] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner of British Columbia, *Getting Accountability Right with a Privacy Management Framework*, 17.4.2012, available at: www.priv.gc.ca/leg_c/interpretations_02_acc_e.asp (last accessed 27.9.2012).

[52] The three phases of the project on accountability are contained in the following documents of Centre for Information Policy Leadership, Hunton & Williams LLP, "Data Protection Accountability: The Essential Elements. A Document for Discussion", October 2009, http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf; "Demonstrating and Measuring Accountability: A Discussion Document. Accountability Phase II – The Paris Project", October 2010, http:// www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF; „Implementing Accountability in the Marketplace: A Discussion Document. Accountability Phase III - The Madrid Project", November 2011, http://www.hunton.com/files/Uploads/Documents/Centre/Centre_Accountability_Phase_III_White_Paper.pdf. Currently ongoing (during 2012) is phase IV of this project. For more detailed information on the project and ongoing work, see the webpage of the Centre for Information Policy Leadership: http://www.informationpolicycentre.com/accountability-based_privacy_governance/.

business sense in the first place), they will most likely be caught by proposed new rules[53].

As to the objective to guarantee equivalent levels of data protection EU-wide, in addition to the previously explained intention of the Commission to have the new rules adopted in the form of a regulation, such aim is visible also from the proposed territorial scope of Regulation, which would also extend to certain processing operations by controllers who are not established in the EU. Thus the new rules are intended also to apply to processing of personal data of data subjects residing in the EU by controllers not established in the EU, where their processing activities relate to offering of goods or services to these data subjects
(EU residents), or to monitoring of their behavior[54].

A further intention of proposed Regulation is to more clearly allocate and affirm data protection responsibility and liability to all those who are effectively in charge of personal data processing. While such responsibility was so far mostly reserved for "data controllers" who determine the purposes, conditions and means of personal data processing, alone or jointly with others[55], proposed new rules aim for a clearer attribution of responsibility[56] especially taking into account more complex data processing environments that are particularly manifest in the online environment, *e.g.* cloud computing[57]. Thus aside from the classic scenario of one data controller and a data controller-data processor relationship where the processor processes personal data on behalf of (and upon instructions of) the controller[58], the Proposal introduces also the scenario of „joint controllers" (jointly established purposes, conditions and means of processing personal data[59]) and also establishes their joint responsibility. Joint controllers would be obliged to establish and mutually arrange their respective responsibilities for compliance with relevant duties, and especially as to procedures and mechanisms for exercising various data subjects' rights[60]. This arrangement will need to be meticulously considered, especially taking into account proposed severe administrative fines also for cases when the relevant controller(s) does not *sufficiently* determine respective responsibilities with the co-controllers[61].

---

[53] See Art. 4. paras. 1-2. and recitals 23-24. of the Proposal. Additionally, see an extensive opinion of the Working Party: *Opinion 4/2007 on the concept of personal data*, 01248/07/EN, WP 136, 20.6.2007.
[54] Article 3 of the Proposal, additionally see recitals 20-22. of the Proposal.
[55] Article 4. para 5. of the Proposal.
[56] See recital 62. of the Proposal.
[57] See, e.g. the opinion of the Article 29 Working Party on the issue: *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN, WP 169, 16.2. 2010., as well as: European Commission, *op. cit*. at note 12 (Annex 2 to the Impact Assessment), section 10.1.2.
[58] Article 4. para. 6 of the Proposal.
[59] Article 24. of the Proposal.
[60] Article 24. of the Proposal.
[61] See Article 79. para. 5 of the Proposal.

The other new scenario envisaged in the Proposal is where processors process data beyond controller's instructions, which are then considered joint controllers with respect to such processing and are therefore subject to the aforementioned rules on joint controllers.[62] A clearer attribution of responsibility for all those who are effectively in charge of data processing in the Proposal has also resulted in more extensive data protection obligations for „classic" data processors.[63] In fact, certain elements of data controller's accountability are also extended to data processors, such as, for example, the duty to keep and maintain documentation on personal data processing and present it on request to the data protection supervisory authority[64] and the duty to co-operate with the authority[65], as well as the duty to appoint a data protection officer[66].

Described new elements for allocation of responsibility as well as a set of reinforced obligations on the part of data processors are reflected also in the proposed liability regime for damages, given that apart from liability of the data controller, also the processors' liability is introduced by the Proposal. Hence a person suffering damages as a result of unlawful processing or other action that is not in line with proposed Regulation would have the right to receive compensation from the controller, or the processor. Furthermore, a liability regime of joint and several liability for the entire amount of damage is proposed for anticipated scenarios with joint controllers or with multiple processors engaged in data processing. Exemption from such liability would be possible in cases where the controller or processor can prove they are not responsible for the event giving rise to the damage[67].

With respect to the previously examined tasks of the Working Party, it should be noted that the Proposal reinforces it and renames into a „European Data Protection Board", which is to be in charge of ensuring consistent application of the Regulation. Certain changes are proposed as to its membership and the secretariat would no longer be provided by the Commission, but by the EDPS[68]. The Board would have a stronger coordinatory role with respect to national supervisory authorities. As regards mutual co-operation between the national data protection authorities, the Proposal introduces mechanisms to ensure their stronger and more effective co-operation[69]. In addition to this, the objective of uniformity in application and effective enforcement of data

---

[62] See Article 26. para. 4. in connection with Article 24. of the Proposal.
[63] As one example, see Article 26. para. 2. of the Proposal.
[64] For more details, see Article 28. of the Proposal (in relation to data controller's accountability in this area, see Article 22. para. 1. and 2a of the Proposal).
[65] Article 29. of the Proposal.
[66] See Articles 35-37. of the Proposal.
[67] Art. 77. of the Proposal.
[68] The Commission (representative of) is no longer to be a member (of the future Board), although it retains the right to participate in its activities and be represented, *i.e.* as an observer. For more details on the Board, proposed consistency mechanisms, a reinforced coordinatory role of the Board with respect to national data protection authorities as well as details on enhanced mutual cooperation, see Chapter VII. of the Proposal.
[69] For details, see in particular Chapter 7. of the Proposal.

protection EU-wide is complemented in the Proposal by important provisions on independence and powers of data protection authorities[70] - key elements of successful data protection systems, but on which Member States' data protection laws largely diverge from each other.

I will here highlight the proposed rules empowering data protection authorities to *directly impose administrative fines*, taking into account that this is (in addition to other proposed rules on liability and remedies) an area that has an eye-catching effect as to the newly proposed legal-regulatory framework in general, especially in terms of legal risk management. Thus apart from the stated powers of data protection supervisory authorities to issue fines directly, the Proposal also introduces requirements on sanctions, which must in each individual case be effective, proportionate and dissuasive. Also specified are the criteria for establishing the amount of the fine and these are: nature, gravity and duration of breach (as well as intentional or negligent character thereof), degree of a person's responsibility and their previous breaches (if any), technical and organizational measures and procedure implemented to fulfill the duty of data protection by design and default, and the degree of cooperation with the data protection authority in order to remedy the breach. With certain exceptions, three categories of monetary fines for intentional or negligent violations of the Regulation are set out in the Proposal[71].

Particularly important in light of the topic of this paper are fines envisaged for breach of reinforced accountability obligations, which for the most part (but not exclusively) fall in the most severe category where fines can rise up to EUR 1 000 000, or up to 2 % of the annual worldwide turnover in case of an enterprise[72]. This is, for example, proposed for cases of (intentional or negligent) failure to adopt internal policies or implement appropriate measures for ensuring and demonstrating compliance, failure to undertake a data protection impact assessment, processing personal data without prior authorization or consultation of the data protection authority (when required), as well as a failure to designate a data protection officer (or even in cases when prescribed conditions for fulfilling this officer's tasks have not been met).[73] In addition, also non-compliance with specific personal data breach notification duties, which I will explain in the next section of this paper, would fall under this most severe fine category. Interestingly, while the lack of measures for ensuring and demonstrating compliance with data protection rules is proposed as one of the strictest violations, which contains also a requirement to implement such measures with

[70] See Chapter 6 of the Proposal for more details. As to requirements on independence of data protection supervisory authorities in the practice of the Court of Justice of the EU, see: C-518/07 European Commission v Federal Republic of Germany, Court of Justice of the European Union, 9.3.2010, European Court reports 2010, p. I-01885, in particular paras. 17-56.

[71] See Art. 79. para. 3., Art. 79. paras. 4-6. of the Proposal.

[72] An enterprise is defined as any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity (Article 4. para. 15. of the Proposal).

[73] Art. 79. para. 6 e, 6 i, 6 j. of the Proposal.

respect to the duty to keep documentation, failure to keep documentation (or even failure to *sufficiently maintain* it) is itself introduced as a less severe (but still very significant) violation[74]. In case of intentional or negligent breach of this duty to keep documentation, proposed maximum fine amounts to up to EUR 500,000, or up to 1% of the annual worldwide turnover of an enterprise[75].

The other particularly eye-catching element in terms of legal risk management for organizations is the newly introduced right of *collective redress*. Namely, any lawfully constituted body, organization or association aiming to protect data subjects' rights and interests with respect to personal data protection would have the authority to initiate the relevant administrative procedure before a data protection authority, as well as court proceedings. Such organizations would have the right to lodge a complaint with the supervisory authority on behalf of data subjects if they consider their relevant rights were violated as a result of personal data processing, but also on their own behalf, *i.e.*, independently of a data subject's complaint, if they consider that a personal data breach occurred.[76] They would also have the right to a judicial remedy on behalf of data subject(s) not only against the controllers, but also processors as well as the supervisory authority[77].

4. Elements of reinforced data protection accountability

A firm requirement of reinforced accountability as one of the principles relating to personal data processing is introduced in Article 5f of the Proposal, according to which personal data must be processed under the responsibility and liability of the controller, who must ensure and demonstrate compliance with the Regulation for each processing operation.[78] Controller's main responsibility in this sense is, according to Article 22 of the Proposal, adopting policies and implementing appropriate measures to ensure and be able to demonstrate that the processing is carried out in compliance with the Regulation. The Proposal also set outs five key examples of measures that must be taken in order to implement this duty, and these are, as follows: keeping of documentation on processing operations, implementing data security requirements, performing a data protection impact assessment, complying with requirements on prior authorization or prior consultation of the data protection supervisory authority, and appointing a data protection officer. The controller is also obliged to implement mechanisms to ensure that effectiveness of these measures is verified, which may be enforced via audits (independent internal or external auditors), if proportionate.

---

[74] Art. 79. para 5 f. of the Proposal.
[75] Art. 79. para 5 f. of the Proposal.
[76] Art. 73. paras. 2-3. of the Proposal.
[77] Art. 76 para. 1 in relation to Arts. 73 and 74. of the Proposal.
[78] See also recital 60. of the Proposal, which states that comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate compliance of each processing operation with the Regulation.

The first of the listed accountability measures is *keeping of documentation of processing operations under the controller's responsibility.* In an overview of reinforced duties of processors I already pointed to the fact that this duty is proposed to also be imposed on the processors. The duty requires, essentially, that the controller (and processor, and if any, controller's representative) maintains documentation of all processing operations under its responsibility and that this documentation is made available to the data protection authority on request, since it would be used for monitoring those processing operations.[79] The core, minimum documentation that must be kept (in the example for controller) is: its name and contact details and (if any) of the data protection officer, purposes of processing, categories of data subjects and their personal data, recipients or categories of recipients of personal data, transfers of data to a third country or international organization (and documentation of safeguards in a particular case), a general indication of time limits for erasing different data categories. Final obligatory element is a description of mechanisms to ensure verification of effectiveness of measures that have been implemented, in order to fulfill its accountability obligation (to ensure and demonstrate compliance with the Regulation)[80].

As to controllers the described obligation to keep documentation is intended to replace their duty to notify processing activities to the supervisory authority in accordance with Articles 18(1) and 19 of Directive 95/46/EC. The documentation that must be maintained corresponds to a certain extent to the documentation that must be provided to the data protection authority for the purpose of notifying processing operations in accordance with Directive 95/46/EC. With that in mind, it should be noted also that this directive itself provides for options when Member States may simplify, or even exempt the controllers from this notification duty (including instances where the controller appointed a data protection officer). The Proposal envisages as exemptions from the duty to keep documentation only the following two cases: where natural persons process personal data without a commercial interest, and where enterprises or organizations with less than 250 employees process personal data only as ancillary activity to their main activities.

In any case, with introduction of a comprehensive documentation keeping duty, Article 18 of Directive 95/46/EC on notification is proposed to be abolished by the Regulation and according to the Commission's impact assessment, that was appraised to „greatly simplify the regulatory environment, reduce administrative burden and increase the consistency of enforcement“[81], which is nowadays especially cumbersome (and costly) for controllers operating in several Member States, which must notify processing operations in each of these countries. However, taking into account that by its scope the proposed new duty to keep documentation is by now already widely criticized especially due to

[79] Article 28 of the Proposal, also see clarifications in recital 65.
[80] Art. 28. para. 1. of the Proposal.
[81] European Commission, *op. cit*. at note 12, p. 72 (point 6.1.3. a).

its own, in the least administrative burdens for affected persons and entities, the extent of attenuation in a likely revision, remains to be seen.

In certain cases the duty to notify processing to the data protection authority has not been abolished (prior checking[82]), and remains applicable for specific cases where processing operations are likely to present specific risks to rights and freedoms of data subjects.[83] In fact, complying with the newly proposed requirements for prior authorization and consultation of data protection authority is also introduced as one of the key accountability measures.[84] In that sense, the controller's intended data processing requires *prior authorization* from the data protection supervisory authority in certain cases of transfers of personal data to a third country or an international organization. The other proposed mechanism, *prior consultation* of the data protection authority is intended for other specific cases where processing operations are likely to present specific risks for data subjects, such as, *e.g.*, where a performed data protection impact assessment showed a high degree of such risk.

Risk assessment procedures such as privacy impact assessments are indispensable tools for ensuring early identification of possible risks for individuals' rights and freedoms, such as in particular their privacy and personal data protection rights, and for managing such risks. According to research privacy impact assessments are beneficial, for example, in terms of reduction of costs in management time and legal expenses, and the overall avoidance of "costly or embarrassing privacy mistakes"[85]. The Proposal introduces a duty to carry out such impact assessments as an accountability measure, albeit by the name „data protection impact assessments", which could be misleading given the intended broad scope of application of such procedures (in relation to risks presented for data subjects' rights and freedoms[86]). In any case, such data protection impact

---

[82] Art. 20. of Directive 95/46/EC. Prior checks according to this directive could also be performed by the data protection officers, if appointed by the controller, and they are obliged to consult the data protection supervisory authority in cases of doubt.

[83] Article 34. of the Proposal.

[84] Art. 34. paras. 1-2. of the Proposal in connection with Article 22 para. 2 d. of the Proposal.

[85] PIAF consortium (eds. Dariusz Kloza *et al.*), *PIAF - A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable D1*, 21.9.2011, available at: http:// www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf, last accessed 27.9.2012 (citation at pp. 20, 185); David Wright, *The state of the art in privacy impact assessment*, "Computer Law & Security Review", Elsevier, Vol. 28, Issue 1, 2012, pp. 54-61 (citation at p. 55). Privacy impact assessment considerations are today in advanced stage for the specific area of RFID, for more details see the industry framework: *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 12.1.2011, available at: http://ec.europa.eu/ information_society/policy/rfid/documents/infso-2011-00068.pdf (last accessed 27.9.2012) and example of a guideline-tool: Bundesamt für Sicherheit in der Informationstechnik, *Privacy Impact Assessment Guideline for RFID Applications*, 2011, available at: https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/PIA/pia_node.html (last accessed 27.9.21012).

[86] For interesting discussions on the proposed impact assessment, see: Luiz Costa, Yves Poullet, *op. cit.* at note 30, p. 260; Paul De Hert, Vagelis Papakonstantinou, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*,

assessments must be conducted by controllers, as well as processors when acting on their behalf, in special cases where data processing entails specific risks to data subjects' rights and freedoms (by virtue of their nature, scope or purposes). In short, provided examples of especially risky operations in the mentioned sense include: personal data in large scale filing systems on children, genetic data or biometric data; processing operations with certain other sensitive data for specific purposes, certain „profiling" operations, in the sense of systematic and extensive evaluation of personal aspects relating to individuals or for analyzing or predicting in particular their economic situation, location, health, personal preferences, reliability or behavior; monitoring publicly accessible areas and, of course, other processing operations with respect to which the controllers (or processors acting on their behalf) have a *duty of prior consultation* with the data protection authority[87]. At minimum the data protection impact assessment must contain a general description of processing operations, assessment of risks for data subject's rights and freedoms as well as the intended measures to address risks, safeguards, security measures and mechanisms to ensure personal data protection and demonstrate compliance with the Regulation.

Implementation of personal *data security* requirements is another explicitly stipulated accountability measure in the Proposal. Security requirements are according to Article 30 of the Proposal binding on both the controller and the processor, regardless of its contractual arrangement with the controller[88], and according to them they must implement appropriate technical and organizational measures (having regard to state of the art and costs of their implementation) to ensure a security level appropriate to risks that the processing represents, and to the nature of protected personal data. Moreover, following risk evaluation, the controller and the processor must take these measures to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access, or alteration of personal data. These security requirements are especially important in the context of new procedures and obligations in relation to *personal data breaches*.

The Proposal has introduced a definition of a personal data breach and breach notification procedures[89], largely based on data breach provisions in the amended Directive 2002/58/EC concerning the processing of personal data and

„Computer Law & Security Review", Elsevier, Vol. 28, Issue 2, 2012, pp. 130-142 at pp. 140-141.

[87] As further explained in relevant recitals, the duty to perform data protection impact assessments should in particular apply to newly established large scale filing systems that aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects, and in connection with a prior consultation duty, where individuals would, *e.g*., be excluded from their right, etc. See Art. 33. of the Proposal for more details on proposed data protection impact assessment requirements, and additionally (also in connection with the prior consultation duty) recitals 70-74. of the Proposal.

[88] European Commission, *op. cit*. at note 3, p. 10.

[89] Article 4. para. 9., Articles 31-32. of the Proposal. Additional explanations are provided in recitals 67-69 of the Proposal.

the protection of privacy in the electronic communications in 2009.[90] A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. The controller is obliged to notify the data breach to data protection supervisory authority without undue delay, and, where feasible, not later than 24 hours after having become aware of it. Apart from the duty to notify this authority, it would also be required to notify the data subjects themselves in cases where the breach is likely to adversely affect the protection of data subject's personal data or privacy. In such cases it is proposed that the controller must notify the data subject without undue delay, after it has notified the data protection supervisory authority. In all cases where the processor processes data on behalf of controller, the processor's duties in case of a personal data breach need to be covered in the relevant contract (or other legally binding act) with the controller[91]. This is so especially taking into account the proposed duty of processor to alert and inform the controller immediately after establishing the data breach[92]. Earlier I pointed to proposed sanctions in cases of intentional or negligent noncompliance with the data breach notification duties (including the stated duties of processor vis-à-vis the controller) is considered as a severe violation of the Regulation, for which the supervisory authority could impose a maximum administrative fine[93].

It could be said that implementing the next two principles into a set of binding obligations signifies acknowledgment of intrinsic technological foundations of efficient personal data protection in the post-modern digital age, and these are *data protection by design* and *data protection by default*.

The duty to apply them in practice as such represents a relevant accountability measure: "in order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default[94]. Their concept draws on the already well-known principle of *privacy by design* in data protection globally[95], which together with use of privacy enhancing technologies provides for consideration of

---

[90] Article 2h and Article 4. para. 3 of Directive 2002/58/EC. These rules were enacted with the amendment of this directive in 2009 (Art. 2. para. 2c and Art. 2. para. 4c of Directive 2009/136/EC).

[91] See especially Article 26. para. 2f and 2 h, and Article 26. para. 3. of the Proposal.

[92] Article 31. para. 2. of the Proposal.

[93] Article 79. para. 6h. of the Proposal. For exceptions, see Article 79. para. 3. of the Proposal.

[94] Recital 61. of the Proposal. For more details on duties of data protection by design and by default, see Article 23. of the Proposal.

[95] For more details, see: Ann Cavoukian, *Privacy by design … take the challenge*, Information and Privacy Commissioner of Ontario, Canada, January 2009, available at: http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf (last accessed 27.9.2012); *Privacy by Design Resolution*, 32nd International Conference of Data Protection and Privacy Commissioners, 27-29.10.2010, Jerusalem, Israel, available at: http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf (last accessed 27.9.2012).

measures and controls needed to efficiently enforce relevant data protection principles (especially minimization of data and purpose limitation), and for their embedding into data processing systems as early in the design process, up to the end of the relevant lifecycle. Hence the duty to apply *data protection by design is* proposed already at the time of establishing means of processing data, as well as during processing itself, and consists of adequate technical and organizational measurers and procedures (with regard to the state of the art, as well as costs of implementation) that are necessary to ensure compliance of data processing with the Regulation. Implementing *data protection by default* signifies certain core data protection principles, such as data minimization. This means that by default only necessary personal data should be processed (with respect to each specific processing purpose). Moreover, as regards the amount of data and time of their storage, they must not be collected or retained beyond the minimum necessary for those purposes. A specific example of violation of this principle is where personal data are set by default to be accessible to indefinite number of individuals.

Designation of a „data protection officer" is in my opinion a crucial accountability measure, which has already been introduced by Directive 95/46/EC, in basic terms, as the data controller's voluntary measure[96]. With detailed provisions on appointment, position and tasks[97] the Proposal introduces mandatory appointment of the data protection officer not only by the controller, but also the processor, in case of a public authority or body (which is carrying out personal data processing) or an enterprise (any entity engaged in an economic activity, irrespective of its legal form) with 250 or more employees, and in cases where controller's or processor's core activities include processing operations requiring regular and systematic monitoring of data subjects. At minimum the officer's tasks must include: informing and advising the controller (or processor) of his/her obligations under the Regulation and documenting this activity as well as responses; monitoring implementation and application of controller's (or processor's) data protection policies (including assignment of responsibilities, training of staff and audits), monitoring implementation and application of the Regulation (especially as regards requirements on data protection by design and by default, data security, information of data subjects and their requests in exercising their rights); ensuring maintenance of documentation on all processing

[96] According to Directive 95/46/EC a data protection official can be appointed by the controller, and he or she would in particular be responsible for ensuring, in an independent manner, internal application of national data protection laws, as well as for keeping the register of processing operations. See especially Art. 18. para. 2. and recital 49. Directive 95/46/EC. It should be noted also that according to Regulation No. 45/2001 all bodies and institutions of the EU must have an appointed data protection officer. See Art. 24. para. 1., and additionally, guidelines from the EDPS: European Data Protection Supervisor, *Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8),* 29.7.2010, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-29_Guidelines_DPO_tasks_EN.pdf (last accessed 27.9.2012).

[97] See section 4 of the Proposal (Articles 35-37) for more details.

operations and monitoring documentation, notification and communication of personal data breaches; monitoring performance of controller's (or processor's) data protection impact assessment and applications for prior authorization or consultation, as well as monitoring responses to requests from the data protection authority, co-operating with it and acting as its contact-point.

Taking into account the distinctive role and all-round duties and tasks towards ensuring internal compliance, the Proposal also introduces controllers' and processors' duty to support the data protection officer in performing his or her tasks and to ensure these duties and tasks are performed independently, and without any instructions. Moreover, they must ensure that the data protection officer is properly and in a timely manner involved in all issues relating to personal data protection. The data protection officer is to directly report to the management.

In relation to all examined accountability measures it is important to make a reference here also to proposed duty of Member States and the Commission, which aims towards ensuring transparency on demonstrated compliance as regards products and services. Namely, it would be their duty to encourage establishment of *certification mechanisms, data protection seals and marks*[98].

5. Concluding remarks

Even though the legislative process for the new EU general data protection legal-regulatory framework is presently underway and it is likely that some of the more progressive measures proposed towards an all-round legally enforceable accountability, which I analyzed in this paper, could be adopted differently than proposed, or even dropped, I do not consider that the key motivation for their introduction would vanish from the finally adopted text altogether. In fact, in my opinion most if not all examined obligations in this direction are logical attempts to establish a more orderly, actual, reliable and therefore categorical data protection compliance, primarily in the organizational sense. This would in turn enable supervisory authorities and data subjects and, in the first place responsible entities themselves, to more effectively cope with the challenges in the increasingly ubiquitous and technologically-induced area of personal data protection in the post-modern digital age. The main goal of this paper was, therefore, to analyze key motivations for introducing advanced legal-regulatory means towards demonstrable compliance or, in other words, the reactive evolution of a unique law of accountability in data protection, which marks an enterprising step forward in relation to the more typical self-regulated accountability.

Aside from legal risks and consequences, mere reputational damage of bad press with the growingly extensive media coverage of bad practices in data protection will only add up to commitments toward better enforcement of the

[98] Article 39 of the Proposal.

law, in light of increasing awareness of individuals themselves of their rights and risks to their rights. Apart from this, expansion of organizations and associations promoting and defending privacy rights will additionally foster the already noticeably proliferating data protection industry in general. It is, therefore, high time for organizations handling personal data and especially those with a central business focus around data management, as well as those processing such data online, to acknowledge the actual benefits of *preventive compliance* in this area of law. Essentially this means, especially taking into account the very broad scope of application of the law to personal data protection, acknowledging the need for a proper organizational structure, *i.e.*, internal management and governance structure, to introduce and further support internal processes, which are functionally designed to support compliance in the area. Such a structure will be prepared for responses to all relevant data protection requirements, as well as any reinforced accountability measure that may be introduced by the law.

Bibliography

Legislation

1. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, Official Journal of the European Union C 306, 17.12.2007, pp. 1-271.
2. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Official Journal of the European Union C 83, 30.3.2010, p. 47.
3. Charter of Fundamental Rights of the European Union, Official Journal of the European Union C 83, 30.3.2010, pp. 389-403.
4. 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, Official Journal of the European Union L 281, 23.11.1995, pp. 31-50.
5. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Union L 201, 31.7.2002, pp. 37-47.
6. 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, Official Journal of the European Union L 350, 30.12.2008, pp. 60-71.
7. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Official Journal of the European Union L 337, 18.12.2009, pp. 11-36.
8. 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, Official Journal of the European Union L 8, 12.1.2001, pp. 1-22.
9. Convention for the protection of human rights and fundamental freedoms, CETS No. 005, 4.11.1950.
10. Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 28.1.1981.
11. *Personal Information Protection and Electronic Documents Act -"PIPEDA"*, SC 2000, c 5, available at: http://canlii.ca/t/l29k (last accessed 27.9. 2012).

Case Law

1. Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, 09.11.2010, Court of Justice of the European Union, European Court reports 2010, p. I-11063.
2. C-518/07 European Commission v Federal Republic of Germany, Court of Justice of the European Union, 9.3.2010., European Court reports 2010, p. I-01885.

Other Official Documentation

1. Article 29. Data Protection Working Party: *Opinion 4/2007 on the concept of personal data*, 01248/07/EN, WP 136, 20.6.2007.
2. Article 29 Data Protection Working Party, *Report 1/2007 on the first joint enforcement action: evaluation and future steps*, 01269/07/EN, WP 137, 20.6.2007.
3. Article 29 Data Protection Working Party, *Joint Investigation Action on the Implementation of the Data Retention Directive*, Press Release, 10.12.2008, available at: http://ec.europa.eu/justice/policies/privacy/news/docs/pr_17_03_09_en.pdf (last accessed 27.9.2012).
4. Article 29 Data Protection Working Party and 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*, 02356/09/EN, WP 168, 1.12.2009.
5. Article 29. Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor*", 00264/10/EN, WP 169, 16.2. 2010.
6. Article 29 Data Protection Working Party, *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*, 00058/10/EN, WP 172, 13.7.2010.
7. Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, 00062/10/EN, WP 173, 13.7.2010.
8. Asia-Pacific Economic Cooperation (APEC) Privacy Framework, December 2005, APEC Secretariat, Singapore, available at: http://publications.apec.org/publication-detail.php?pub_id=390 (last accessed 27.9.2012.)
9. Bundesamt für Sicherheit in der Informationstechnik, *Privacy Impact Assessment Guideline for RFID Applications*, 2011, available at (last accessed 27.9.21012): https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/PIA/pia_node.html

10. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Final document on the modernisation of Convention 108*, T-PD (2012)04Mos, Strasbourg, 15.6.2012, available at: http://www.coe.int/t/dghl/standardsetting/ dataprotection/TPD_documents/T-PD_2012_04Mos.pdf (last accessed 27.9. 2012).
11. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Final document on the modernisation of Convention 108*, T-PD(2012)04 rev en, Strasbourg, 17.9.2012, available at: http://www.coe.int/t/dghl/standardsetting/ dataprotection/TPD_ documents/T-PD_2012_04_rev_en.pdf (last accessed 27.9.2012).
12. European Commission, *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, Brussels, 4.11.2010.
13. European Commission, *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, 2012/0011 (COD), Brussels, 25.1.2012.
14. European Commission, *Commission Staff Working Paper, Impact Assessment – Accompanying the document 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) and 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*, SEC(2012) 72 final, Brussels, 25.1.2012.
15. European Commission, *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, 2012/0010 (COD), Brussels, 25.1.2012*.
16. European Data Protection Supervisor, *Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8),* 29.7.2010, available at: http://www.edps.europa.eu/ EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-29_Guidelines_DPO_tasks_EN.pdf (last accessed 27.9.2012)
17. European Network and Information Security Agency, *The Article 29 Working Party recommendations, consultations and policy documents*, available at: http://www.enisa.europa.eu/act/rm/cr/laws-regulation/data-protection-privacy/article-29-working-party (last accessed 27.9.2012).
18. Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner of British Columbia, *Getting Accountability Right with a Privacy Management Framework*, 17.4.2012, available at: www.priv.gc.ca/leg_c/interpretations_02_acc_e.asp (last accessed 27.9.2012).
19. Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and Explanatory

Memorandum, available at (last accessed September 27, 2012): http:// www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html
20. *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 12.1.2011, available at: http://ec.europa.eu/information_society/policy/ rfid/documents/infso-2011-00068.pdf (last accessed 27.9.2012).
21. *Privacy by Design Resolution*, 32nd International Conference of Data Protection and Privacy Commissioners, 2729.10. 2010, Jerusalem, Israel, available at: http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf (last accessed 27.9.2012).
22. The Madrid Privacy Declaration - Global Privacy Standards for a Global World, 3.11.2009., 31st annual meeting of the International Conference of Privacy and Data Protection Commissioners, Madrid, 4-6.11.2009, available at: http://thepublicvoice.org/madrid-declaration/ (last accessed 27.9.2012).

Books, Articles and other Documents

1. Ann Cavoukian, *Privacy by design ... take the challenge*, Information and Privacy Commissioner of Ontario, Canada, January 2009., available at: http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf (last accessed 27.9.2012).
2. Centre for Information Policy Leadership, Hunton & Williams LLP, *Data Protection Accountability: The Essential Elements. A Document for Discussion*, October 2009, available at: http:// www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf
3. Centre for Information Policy Leadership, Hunton & Williams LLP, *Demonstrating and Measuring Accountability: A Discussion Document. Accountability Phase II – The Paris Project*, October 2010, available at: http://www.huntonfiles.com/ files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF.
4. Centre for Information Policy Leadership, Hunton & Williams LLP, *Implementing Accountability in the Marketplace: A Discussion Document. Accountability Phase III - The Madrid Project*, November 2011, available at: http:// www.hunton.com/ files/Uploads/Documents/Centre/Centre_Accountability_Phase_III_White_Paper.pdf
5. Luiz Costa, Yves Poullet, *Privacy and the regulation of 2012*, „Computer Law & Security Review", Elsevier, Vol. 28, Issue 3, 2012, pp. 254-262.
6. Paul De Hert, Vagelis Papakonstantinou, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, „Computer Law & Security Review", Elsevier, Vol. 28, Issue 2, 2012, pp. 130-142.
7. Maria Koleva, *Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner: We need our citizens on board*, Brussels, „Europost", 07.9.2012, available online at: http://www.europost.bg/article?id=5331 (accessed 27.9.2012).
8. Douwe Korff, *EC study on implementation of data protection directive - Study Contract ETD/2001/B5-3001/A/49, Comparative summary of national laws*, Colchester – Cambridge: University of Essex, 2002, available at: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf (last accessed 27.9.2012).
9. Douwe Korff, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments - Contract No. JLS/2008/C4/011 – 30-CE-0219363/00-28, Working paper No. 2: Data protection*

laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments, LRDP KANTOR Ltd (Leader) – Centre for Public Reform 20.1.2010, available at: http:// ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf (last accessed 27.9.2012).

10. Christopher Kuner, *European data protection law - Corporate compliance and regulation*, Oxford University Press, New York, 2nd ed., 2007.
11. PIAF consortium (eds. Dariusz Kloza *et al.*), *PIAF - A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable D1*, 21.9.2011, available at: http:// www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf (last accessed 27.9.2012).
12. David Wright, *The state of the art in privacy impact assessment*, "Computer Law & Security Review", Elsevier, Vol. 28, Issue 1, 2012, pp. 54-61.