Selected aspects of proposed new EU general data protection legal framework and the Croatian perspective

Senior assistant – lecturer PhD **Nina GUMZEJ**[1]

Abstract

Proposed new EU general data protection legal framework profoundly affects a large number of day-to-day business operations of organizations processing personal data and calls for significant effort on their part toward the necessary legal-regulatory compliance. In this paper the author examines key legislative developments towards this new EU frame and impact for the Republic of Croatia as the youngest EU Member State. Following introductory overview, legal analysis of draft EU General Data Protection Regulation as proposed by the European Commission and recently adopted amendments by the European Parliament mainly focuses on selected solutions impacting national data protection supervisory authorities. This is complemented with examination of relevant sources of EU law, including the case law of the Court of Justice of the European Union. Assessment of results of this research is next made with respect to prospects of the data protection legal framework of the Republic of Croatia. The paper is concluded with the author's critical overview of analyzed EU proposals impacting national data protection supervisory authorities in light of EU pivotal goals, and de lege ferenda proposals to timely address identified obstacles towards more adequate enforcement of data protection legislation in Croatia.

Keywords: *right to personal data protection, independent supervisory authority, General Data Protection Regulation, Croatian Personal Data Protection Act*.

JEL Classification: K20

1. Introduction

Many organizations EU-wide nowadays invest considerable effort towards meeting compliance with the personal data protection legislation. The overreaching material scope of application of relevant rules is one reason for this, given that a large number of day-to-day activities will entail the so-called *processing of personal data* of individuals. Namely, according to the legal framework of the European Union *personal data* (further also referred to as data) entail any information relating to identified or identifiable natural person, *i.e.* data subject.[2] *Processing* personal data denotes a broad range of operations that can be performed

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

[2] 'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Article 2(a) of 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 (General Data Protection Directive). Additionally see recital 26 of the General Data Protection Directive.

on them, which include but are not limited to collection, storage and erasure of personal data.[3] These concepts subsist also in the online environment.[4] Furthermore, an organization such as, for example, a multinational sportswear company with an EU-wide retail market typically must ensure compliance of data processing operations with the data protection legislation of each respective Member State. Harmonization of national laws has to some extent already been achieved with implementation of *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such dat*a (further: *General Data Protection Directive*).[5] However, better consistency in harmonizing relevant rules in all EU Member States is set to take place with the currently ongoing revision of this directive. In fact, according to current draft text[6], the new EU legal framework on general personal data protection is to be adopted in form of a regulation (*General Data Protection Regulation*).[7] This means that the new rules would apply, unlike the General Data Protection Directive, directly and entirely in all Member States of the European Union, including its youngest member – the Republic of Croatia.

Independent authorities supervising personal data processing and ensuring the protection of rights of individuals are key actors in the EU-wide effective frame mentioned above. This is the reason why I chose to focus main research in this paper, following an introductory overview with respect to developments of the relevant new framework, to selected rules impacting data protection supervisory authorities in European Union Member States. The rules are examined on the basis of current draft text of Regulation[8], which in addition to the initial draft proposal

---

[3] 'Processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Article 2(b) of the General Data Protection Directive, *ibid*. For more details on scope of application, see Article 3 of this directive.

[4] This is acknowledged also in the relevant case law of the Court of Justice of the European Union, see: C-70/10 Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs (SABAM), (2011) European Court Reports, I-11959, paragraph 51; C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers (Sabam) v Netlog NV, (2012) European Court Reports, paragraph 49.

[5] Directive 95/46/EC, *op. cit*. at note 1.

[6] 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; European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Background documents and Compromise amendments (October 21, 2013 - meeting), *Compromise amendments 01 – 29; 30 – 91*, http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131021_1830.htm (last accessed 28.10.2013).

[7] Article 288 of the Treaty on the Functioning of the European Union.

[8] Original Commission's Proposal (2012) and compromise text - adopted amendments by the European Parliament (2013), *op. cit.* at note 5. In the analysis I shall in most cases refer to both the Proposal and amended draft text as constituting current (amended) draft text. However, where amendments by the Parliament are prevailing (e.g. newly added articles and/or new solutions proposed), reference may only be made to its amendments in the current draft text of Regulation.

made by the European Commission (Proposal) also includes most recently, *i.e.* at the time of writing this paper, adopted amendments by the European Parliament.[9] Where applicable, this analysis will be made in a comparative overview to solutions of the General Data Protection Directive. Next I shall examine the general data protection legislative framework of the Republic of Croatia. Here I shall also mainly focus my research on the rules pertaining to the national supervisory authority - Croatian Personal Data Protection Agency. Objective of this analysis is assessment of adequacy and efficiency of the overall general data protection system in light of this authority's role, duties and powers according to Croatian legislation. This will result in identification and further analysis of the challenges facing Croatia, especially in terms of central goals of the proposed EU Regulation. The overall aim of research conducted in this paper is to provide a critical overview of analyzed EU draft rules impacting data protection supervisory authorities, in particular with respect to key objectives of the new EU legal framework, as well as provide *de lege ferenda* proposals to timely address identified obstacles towards more adequate enforcement of general data protection legislation in Croatia.

2. Proposed General Data Protection Regulation: selected aspects

2.1. Introductory overview

Over the last years recognition of the right to personal data protection significantly evolved in European Union law, pursuant to which it is today guaranteed to everyone and has a status of a separate fundamental right (*Treaty on the Functioning of the European Union*[10], *Charter of Fundamental Rights of the European Union*[11]). Entering of the Lisbon Treaty[12] into force in 2009 and abolishment of the EU pillar-structure established legal prerequisites for a reform in the approach towards regulating personal data protection at the level of EU law. In line with the new legal basis[13] a new EU data protection framework is currently

---

9 European Parliament, *op. cit.* at note 5.

10 Article 16 paragraph 1 of the Treaty on the Functioning of the European Union. Consolidated version of the Treaty on the Functioning of the European Union, Official Journal of the European Union C 326, 26.10.2012, p. 47.

11 Article 8 paragraph 1 of the Charter of Fundamental Rights of the European Union, *Official Journal of the European Union* C 326, 26.10.2012, p. 391.

12 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.

13 Article 16 paragraph 2 of the Treaty on the Functioning of the European Union, according to which the European Parliament and the Council shall lay down rules, in the ordinary legislative procedure, which relate to protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities falling within the scope of EU law, and the rules relating to free movement of such data. Compliance with these rules will be subject to the control of independent authorities. For derogations in specific areas such as in particular that of a common foreign and security policy see Article 39 of the Treaty on European Union (Consolidated version 2012, *Official Journal of the European Union C 326*, 26.10.2012) in connection with Article 16 paragraph 2 (last sentence) of

in legislative procedure[14], which also includes the draft General Data Protection Regulation that I am focusing on in this paper. As noted in introduction of this paper, proposed Regulation is intended to replace the General Data Protection Directive. That directive aimed to ensure harmonization of national data protection laws, however, the level of implementation in Member States was in the overall not considered satisfactory in light of prevailing EU objectives.[15]

---

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 326, 26.10.2012, p. 337 at p. 347. As for regulating data protection in the areas of judicial co-operation in criminal matters and police co-operation, see a *Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, ibid* (with respect to the new legal basis in Article 16 paragraph 2 of the Treaty on the Functioning of the European Union).

[14] European Commission, European Parliament, *op. cit.* at note 5; 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/2012/010 final, 2012/0010 (COD), 25.1.2012.

[15] "The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC." Recital 7 of current amended draft text of Regulation, European Commission, European Parliament, *op. cit.* at note 5. For studies and conclusions regarding implementation of the General Data Protection Directive in Member States, see e.g.: Douwe Korff, *EC study on implementation of data protection directive - Study Contract ETD/2001/B5-3001/A/49, Comparative summary of national laws*, University of Essex: Colchester – Cambridge, 2002, http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf; Douwe Korff, LRDP KANTOR Ltd (Leader) - Centre for Public Reform, *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*, 20.1.2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf; LRDP KANTOR Ltd (Leader) - Centre for Public Reform, *Comparative study of different approaches to new privacy challenges, in particular in the light of technological developments, Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28, Final Report*, 20.1.2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf (last accessed 20.10.2013); 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*

In view of continuous advances in technology, globalization and increased processing of personal data online[16], with new EU rules a common legal environment should be established that would on one hand provide legal certainty and adequately support relevant business operations towards fostered growth of the digital single market and free-flowing information, and on the other hand ensure more effective protection of individuals' rights, including enhanced control over the processing of their personal data. While a detailed analysis of proposed Regulation would go beyond the scope of this paper, I would here like to draw attention to four elements of its current draft text, which I consider of vital importance for the overall assessment of subject area. Earlier in the paper I explained that the new EU general data protection legal framework is proposed to be passed in form of a regulation, which means that the new rules would apply directly and entirely in all EU Member States.[17] Next, the new framework is intended toward better adaptation of data protection law and especially enforcement thereof in the overall context of post-modern digital age, which is largely technology-driven. Consequently, the new EU rules target to consistently cover also the data processing activities in the online, networked digital environment and in relevant cross-border operations.[18] Thirdly, according to proposed territorial scope of application new provisions would cover also

execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final, Brussels, 25.1.2012, especially pp. 11-21; *Annex 2 Evaluation of the implementation of the Data Protection Directive*.

[16] According to current draft text of Regulation personal data are any information relating to an identified or identifiable natural person, and identifiable person is one who can be identified, directly or indirectly, especially by reference to an identifier such as a name, an identification number, *location data, unique identifier* or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person. Compare Article 4 points 1-2 and additional explanations in recitals 23-24, in: European Commission, *op. cit.* at note 5, and in: European Parliament, *op. cit.* at note 5. For a current definition in the General Data Protection Directive see *op. cit.* at note 1.

[17] See *supra* note 6.

[18] According to draft Article 1 (*subject matter and objectives*) the Regulation lays down rules relating to protection of individuals with regard to personal data processing and rules relating to free movement of personal data. It protects fundamental rights and freedoms of natural persons, and in particular their personal data protection right. Free movement of personal data in the EU shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to personal data processing. According to draft Article 2 (*material scope*) the Regulation would apply to processing of personal data wholly or partly by automated means, irrespective of the method of processing, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Excluded from its scope of application would be processing of personal data: in the course of an activity falling outside the scope of EU law; by Member States when carrying out activities falling within the scope of Chapter 2 of Title V of the Treaty on European Union (common foreign and security policy); by a natural person in the course of an exclusively personal or household activity (this exemption would apply also to publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons); by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. European Commission, European Parliament, *op. cit.* at note 5.

organizations, *i.e.* controllers and processors[19] that are not based in the EU, should they offer goods or services to data subjects in the EU or monitor them (thereby processing their personal data).[20] Finally, it is important to point to the fact that a number of proposed rules aim to ensure stronger protection of data subjects and accordingly, stricter and legally enforceable responsibility and accountability of those who are in charge of processing their personal data. This entails not only obligations of organizations to implement various policies and measures for establishing and maintaining compliance of their data processing operations with the new EU framework, but also for demonstrating such compliance, most notably to the competent supervisory authority, *i.e.* data protection supervisory authority.[21]

A vital role of supervisory authorities in monitoring data processing and ensuring protection of individuals with respect to processing of their personal data is today acknowledged in the General Data Protection Directive. All EU Member States were obliged to establish one or more public authorities that would be in charge of monitoring, within their respective territories, the application of legislation adopted on the basis of that directive.[22] Furthermore, the duty to establish such supervisory authorities according to international law instruments of the Council of Europe must here also be noted. This duty and role of authorities in ensuring compliance of national laws that give effect to main principles of the *Council of Europe Convention for the protection of individuals with regard to*

[19] According to the General Data Protection Directive a controller is a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law. Processors are defined as natural or legal persons, public authorities, agencies or other bodies that process personal data on behalf of the controller. Article 2 points (d)-(e) of the General Data Protection Directive. For relevant definitions according to draft text of Regulation (which are essentially the same as in the directive), see proposed Article 4 points 5-6, European Commission, European Parliament, *op. cit.* at note 5.

[20] Regulation is proposed to apply to personal data processing in the context of activities of establishment of a controller or a processor in the EU - whether the processing takes place in the EU or not. Furthermore, as noted in the paper, it would also apply to processing of personal data of data subjects in the EU by the controller or processor not established in the EU, where processing activities relate to: a) offering of goods or services (*irrespective of whether payment of data subject is required*) to such data subjects in the EU; or b) monitoring of such data subjects. Regulation would also apply to data processing by the controller not established in the EU, but in a place where Member State's law applies by virtue of public international law. Article 3 (territorial scope), European Commission, European Parliament, *op. cit.* at note 5. Additionally, see explanations in draft recitals 19-21.

[21] See e.g. proposed Article 22 and recital 60, European Commission, European Parliament, *op. cit.* at note 5. For a more detailed analysis by this author (on the basis of draft Proposal of the European Commission), see: Nina Gumzej, *Data Protection for the Digital Age: Comprehensive Effectsof the Evolving Law of Accountability*, „Juridical Tribune", December 2012, Vol. 2, Issue 2, pp. 82-108, also available at: http://www.tribunajuridica.eu/arhiva/An2v2/art7.pdf at pp. 84-110 (last accessed 20.10.2013).

[22] Article 28 paragraphs 1 and 6 of the General Data Protection Directive (these authorities may also be requested to exercise their powers by an authority of another Member State).

automatic processing of personal data (further: Convention 108) are subjects of the relevant *Additional Protocol* to this Convention.[23]

According to the main rules on supervisory authorities in the General Data Protection Directive, apart from the requirement that they exercise their function "with complete independence" (but without further detail as I shall examine later in this paper) Member States are obliged to provide the following minimum set of powers for these authorities: *investigative powers* (e.g. access to all relevant information), *effective powers of intervention* (e.g. ordering data erasure or destruction, imposing a temporary or permanent ban on data processing) as well as the *power to engage in legal proceedings* (when national rules are infringed) *or bring such infringements to the attention of judicial authorities*. Member States must also ensure that the decisions of supervisory authorities are subject to judicial review (appeal before national court). Furthermore, supervisory authorities must be able to hear (process) claims dealing with the protection of data subjects' rights and freedoms as to personal data processing, which can be filed by data subjects or associations representing them and with respect to the same data protection aim they also must have a consultative role in the process of drafting relevant rules or measures in their respective Member States. These authorities must also hear all claims for checks on lawfulness of data processing in particular cases where national rules are adopted, which restrict the scope of certain rights and obligations in the directive. As to possible co-operation between the national authorities in different Member States, the General Data Protection Directive mandates such co-operation especially via exchange of useful information.[24]

On the whole, legal requirements on data protection supervisory authorities in the General Data Protection Directive provide enough discretion for the Member States in terms of implementation into national legislation. This is also supported by lacking specifications and/or details on a number of requirements in the directive. It is not entirely surprising, therefore, that relevant national rules transposing the directive (as to independent status, duties and powers, including enforcement methods) can vary throughout the European Union.[25] In terms of

[23] Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 28.1.1981; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, CETS No. 181, 08.11.2001 - see Article 1.

[24] For more details see Article 28 of the General Data Protection Directive (additionally see also explanations in recitals 62-64).

[25] See e.g. European Commission, *Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive*, COM(2007) 87 final, Brussels, 7.3.2007, p. 5. For detailed studies, see: European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, 2010, http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf; Douwe Korff, *Data Protection Laws in the European Union*, The Direct Marketing Association - New York; Federation of European Direct Marketing Brussels, 2005, pp. 145-168 (Chapter VI); Douwe Korff, *EC study on implementation of data protection* directive, *op. cit.* at note 14, pp. 200-209. Also see: European Commission, *Commission Staff*

proposed new EU framework, such a setting may impede key goals of ensuring equivalent levels of protection of data subjects' rights and free flows of personal data in the EU, including the required consistency in application and supervision of application of the new rules, as well as enforcement thereof. As a result the draft EU general data protection rules aim to ensure that supervisory authorities have equal duties and potent powers, including direct sanctioning authority[26], in all Member States.[27] I shall examine mentioned rules in more detail in the next part of this paper.

2.2. Independent supervisory authorities

Earlier in the paper I drew attention to the requirement of complete independence of data protection supervisory authorities pursuant to the EU General Data Protection Directive. Their independent status according to EU law was also more recently proclaimed in the Treaty on the Functioning of the European Union, and it is also established in the Charter of Fundamental Rights of the EU.[28] It is also a fundamental prerequisite for attainment of main objectives of the future EU legal framework on general data protection (Regulation). As regards requirements of the General Data Protection Directive, the Court of Justice of the European Union (further also as: Court) proclaimed the need to ensure independence equally in all Member States: „ *[…] independence of the supervisory authorities, in so far as they must be free from any external influence liable to have an effect on their decisions, is an essential element in light of the objectives of Directive 95/46. That independence is necessary in all the Member States in order to create an equal level of protection of personal data and thereby to contribute to the free movement of data, which is necessary for the establishment and functioning of the internal market.*"[29] Furthermore, this Court interpreted the meaning of *complete*

Working Paper, *op. cit.* at note 14, especially at pp. 17-18; *Annex 2 Evaluation of the implementation of the Data Protection Directive*, *op. cit.* at note 14 at pp. 41-46.

[26] Compare with earlier pragmatic suggestions of certain experts towards considering a shift of enforcement powers away from supervisory authorities: „There is also a more fundamental question about the - in our view, to some extent incompatible - functions of the DPAs. They are advisers and guides. They are also interpreters of the law - and sometimes even quasi-legislators. They are supposed to be advocates on behalf of data subjects. And they are supposed to be law-enforcers. We feel that this is too much to ask of any single body. One danger is that as regulators, they become "captives" of those they regulate, industry and government agencies in particular. That phenomenon is far from limited to data protection authorities: it has been observed in many modern regulatory bodies. But it too serves to underline the tensions between the different functions of these authorities. […] More generally, we feel (without wishing to prejudge this) that consideration could be given to moving enforcement largely away from the DPAs, to the courts and the prosecuting authorities." LRDP KANTOR Ltd (Leader) - Centre for Public Reform, *Final Report*, *op. cit.* at note 14 at pp. 44-45.

[27] As explained in recital 100, European Commission, European Parliament, *op. cit*. at note 5. Duties and powers (Articles 52-53) will be examined in more detail in section 2.2. of this paper *infra*.

[28] Article 16 paragraph 2 of the Treaty on the Functioning of the European Union, Article 8 paragraph 3 of the Charter of Fundamental Rights of the European Union.

[29] C-518/07 European Commission v Federal Republic of Germany, (2010) European Court Reports 2010 I-01885, paragraph 50.

independence[30] following actions filed by the European Commission against certain Member States for non-fulfilment of their relevant obligations under the General Data Protection Directive. In fact currently another case is pending on same grounds following an action taken by the Commission against a Member State (Hungary).[31] According to the Court, complete independence requires that the supervisory authorities are free from any influence, whether direct or indirect, in their work and decision making[32] and a mere risk of political influence over their decisions would interfere with independent execution of their tasks.[33] The Court also ruled that independence is not solely met with established functional independence of supervisory authorities, where there still exists a possibility of external influence on these authorities.[34]

According to the current draft text of the Regulation each Member State is obliged to provide that one or more public authorities are responsible for monitoring its application and for contributing to its consistent application EU-wide, so as to protect fundamental rights and freedoms of natural persons in relation to their personal data processing and to facilitate free flows of personal data in the Union. These authorities would be obliged to co-operate with each other and the Commission for mentioned purposes.[35] In the overall draft new rules on supervisory authorities draw on, and build on relevant solutions of the General Data Protection Directive and where applicable they incorporate interpretations of the Court of Justice of the EU, as well as certain solutions of *Regulation No 45/2001 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* (further: Regulation 45/2001), notably with respect to independent status and powers.[36] Thus, with reference to independent status, draft text of General Data

[30] Article 28 paragraph 1 of the General Data Protection Directive.

[31] C-518/07, *op. cit.* at note 28; C-614/10 European Commission v Republic of Austria, 16.10.2012 (not yet published - text of judgment is available at: http://curia.europa.eu). The currently pending case before the Court of Justice of the European Union on independence of data protection authorities is an action filed by the European Commission against Hungary, which is seeking a decision against Hungary on failing to fulfil its obligations under the General Data Protection Directive. Namely, the earlier Data Protection Commissioner of Hungary was removed from office before end of his term, solely on account of Hungary's re-organization of that office. C-288/12 European Commission v. Hungary, Official Journal of the European Union C 227, 28.07.2012, pp. 15-16; European Data Protection Supervisor, *EDPS pleading Commission v Hungary (C-288/12)*, 15.10.2013, https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Court (last accessed 28.10.2013). Additionally, see: András Jóri, *The End of Independent Data Protection Supervision in Hungary – A Case Study*, in: Serge Gutwirth; Ronald Leenes; Paul De Hert, Yves Poullet (Eds.), *European Data Protection: Coming of Age*, Springer, 2013, pp. 395-406.

[32] C-518/07, *op. cit.* at note 28, see especially paragraphs 17-56 for more details.

[33] C-518/07, *op. cit.* at note 28, paragraph 36.

[34] C-614/10, *op. cit.* at note 30, see especially paragraphs 42 *et seq*.

[35] Article 46 paragraph 1, European Commission, European Parliament, *op. cit*. at note 5.

[36] European Commission, *op. cit*. at note 5, pp. 12-13; Regulation No 45/2001 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,

Protection Regulation stipulates that supervisory authorities must act with complete independence and this also entails duties of their members not to seek or take instructions from anybody, and to refrain from any action that is incompatible with their duties. Any financial control they would be subject to is not to affect their independence, and they must have separate annual budgets.

Members of the supervisory authority, who are to be appointed either by the parliament or government of the relevant Member State, should be persons whose independence is beyond doubt and who have demonstrated experience and skills required to perform their duties - notably in personal data protection.[37] To that effect the draft text as amended by the European Parliament clarifies, in a recital, that the prescribed requirements for their election need to especially stipulate appointment by the parliament or government of the Member State *taking due care to minimise possibility of political interference*, and include rules on their personal qualification, *avoidance of conflicts of interest* and their position.[38] Factors that may prompt dismissal of members of supervisory authorities are serious misconduct on their part and cases where they no longer fulfil the conditions required for performance of their duties, and removal from office would be prompted by term expiry, resignation or compulsory retirement.

Duties of supervisory authorities according to proposed new EU rules, *i.e.* Regulation include[39] the monitoring of and ensuring application of the Regulation, promoting public awareness[40], advising data subjects (on request) and hearing and processing complaints (matter investigation). Complaints can be filed by data subjects (who feel that their rights according to the Regulation have been infringed) as well as bodies, organisations or associations acting in public interest. The latter would be able to act either on behalf of data subjects (should they feel that the data subjects' rights were infringed) or on their own motion (should they consider that the Regulation was violated).[41] Investigations would be carried out on the basis of

---

12.1.2001, pp. 1-22. This Regulation established, *inter alia*, the European Data Protection Supervisor (EDPS) as an independent supervisory authority that is in charge of ensuring respect for the right to personal data protection and privacy in the institutions and bodies of the EU (pursuant to this Regulation).

37 For more details see Articles 47-48, European Commission, European Parliament, *op. cit.* at note 5.

38 Recital 95, European Commission, European Parliament, *op. cit.* at note 5.

39 For a full list see Article 52, European Commission, European Parliament, *op. cit.* at note 5.

40 According to current draft text of Article 52 paragraph 2 (European Commission, European Parliament, *op. cit.* at note 5), each supervisory authority shall promote awareness of the public on risks, rules, safeguards and rights in relation to personal data processing and on appropriate data protection measures, with specific attention requested on activities addressed to children. Additionally, according to proposed Article 52 paragraph 2a (European Parliament, *op. cit.* at note 5), each supervisory authority is to promote, together with the European Data Protection Board (independent body in charge of ensuring consistent application of the Regulation), awareness of controllers and processors on risks, rules, safeguards and rights in relation to personal data processing, which includes keeping a register of sanctions and breaches. Furthermore, all supervisory authorities would be obliged to provide micro, small and medium sized enterprise controllers and processors on request with general information on their responsibilities and obligations in accordance with the Regulation.

41 Article 73 paragraphs 2-3, European Commission, European Parliament, *op. cit.* at note 5.

complaints or on supervisory authorities' own motion, as well as on request of another supervisory authority.[42]

The context of cross-border personal data processing operations, including online data transfers, triggers in particular the need for prescribing enhanced duties of co-operation between the data protection supervisory authorities and their mutual assistance (including joint investigative tasks and enforcement measures).[43] The key objective of ensuring consistency in application and enforcement of the Regulation in the EU calls *inter alia* for obligatory co-operation between supervisory authorities themselves and the European Commission, via a particular procedure (so-called *consistency mechanism*)[44], and the participation of supervisory authorities in activities of the *European Data Protection Board*.[45] It goes without saying that mentioned duties support proposed benefits for controllers and processors with data processing operations in several Member States, such as the supervision of these operations by the authority of Member State of their main establishment, *i.e. lead authority* (inclusive of required consultations with other competent authorities)[46] as well as benefits for data subjects, such as the right to file a complaint with the supervisory authority in any Member State (and thus also the authority of their country of residence).[47]

Draft text of the Regulation introduces particular tasks and powers of supervisory authorities with respect to processing operations that are likely to present specific risks to rights and freedoms of data subjects (*prior consultation*). These build on current solutions on the so-called *prior checks* in the General Data Protection Directive.[48] Namely, data protection authorities would be authorized to

---

42 Article 52 paragraph 1d, European Commission, European Parliament, *op. cit.* at note 5.

43 Recital 91, European Commission, European Parliament, *op. cit.* at note 5. To compare with objectives and current solutions according to the General Data Protection Directive, see especially Article 27 paragraph 6 thereof, and explanations in recital 64.

44 Draft rules on co-operation and consistency are laid out in Chapter VII, European Commission, European Parliament, *op. cit.* at note 5 (taking into account amendments to the original Proposal). For details on proposed consistency mechanism see especially Articles 57-61, European Commission, European Parliament, *op. cit.* at note 5. Additionally see also Article 46 paragraph 1.

45 The European Data Protection Board is envisaged to be an independent body in charge of ensuring consistent application of the Regulation, whose members would be the European Data Protection Supervisor and heads of EU Member States' data protection supervisory authorities (one per Member State). For more details see Chapter VII Section 3 (Article 66 especially with respect to tasks of the Board), European Commission, European Parliament, *op. cit.* at note 5. The Board is to replace the current *Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data* (Article 29 Data Protection Working Party), whose members are representatives of data protection supervisory authorities of EU Member States, European Data Protection Supervisor and a representative of the European Commission (see Articles 29-30 of the General Data Protection Directive for more details).

46 For more details on proposed mechanism of co-operation with the lead authority, as well as the relevant role of the European Data Protection Board see especially Article 54a (additionally see also explanations in recitals 97-98a), European Parliament, *op. cit.* at note 5. A definition of main establishment is laid out in draft Article 4 point 13, European Parliament, *op. cit.* at note 5.

47 Article 73 paragraph 1, European Commission, European Parliament, *op. cit.* at note 5.

48 Article 20 and Article 28 paragraph 3 (powers of intervention) of the General Data Protection Directive.

prohibit any such data processing that is in contravention of the Regulation, as well as advise on steps towards meeting necessary compliance.[49] Further empowerments that also build on solutions in the General Data Protection Directive include the power to notify judicial authorities of violations of the Regulation, and the power to engage in legal proceedings.[50] As regards the latter[51] I would especially draw attention to the possibility that the supervisory authority of data subject's habitual residence may decide to bring judicial proceedings, on prior request and on behalf of the data subject, against another supervisory authority (e.g. that of a Member State where the controller in question has main establishment).[52]

Supervisory authorities would in line with the General Data Protection Directive continue to have a considerable consultative role also according to draft Regulation, with respect to administrative and legislative measures relating to personal data protection in their respective Member States.[53] Particularly pertinent for this task (but also for many other tasks of supervisory authorities under the draft Regulation) is the introduced duty of *mandatory monitoring of developments relevant to personal data protection, and especially development of information and communication technologies and commercial practices*.[54]

Special emphasis in current draft text of Regulation is placed on the role of supervisory authorities with respect to *certifications* of controllers and processors as to compliance of their personal data processing with the Regulation (*European*

---

[49] For more details on tasks and powers with respect to prior consultation see Article 52 paragraph 1g and Article 53 paragraph 1d in connection with Articles 34 (and 33), European Commission, European Parliament, *op. cit.* at note 5.

[50] Article 53 paragraph 3, European Commission, European Parliament, *op. cit.* at note 5. Article 28 paragraph 3 of the General Data Protection Directive specifies the power to engage in legal proceedings where there was infringement of national rules implementing that directive, *or* the power to bring such violations to the attention of judicial authorities.

[51] Article 53 paragraph 3 in relation to Article 74 paragraph 4 and Article 75 paragraph 2, European Commission, European Parliament, *op. cit.* at note 5.

[52] Article 53 paragraph 3 in relation to Article 74 paragraph 4, European Commission, European Parliament, *op. cit.* at note 5. According to explanations in proposed recital 115 such case could be where the supervisory authority has not acted or took insufficient measures with respect to data subject's complaint. It should here also be noted that such course of action according to current amended draft text (European Parliament) would be without prejudice to the consistency mechanism.

[53] Article 28 paragraph 2 of the General Data Protection Directive, Article 52 paragraph 1f, European Commission, European Parliament, *op. cit.* at note 5. Furthermore, consultative role of authorities (Member States' duty to consult them) is proposed to apply mandatorily in cases of potentially risky data processing operations for data subjects (by virtue of their nature, scope and/or purpose), *i.e.* when legislative measures (or measures based on them) are drafted that define the nature of data processing, especially in order to manage or minimize risk(s) for affected individuals. Article 52 paragraph 1g, Article 34 paragraph 7 and recital 74, European Commission, European Parliament, *op. cit.* at note 5 - compare with Article 20 paragraph 3 of the General Data Protection Directive, according to which Member States *may* carry out prior checks in the context of preparation of such measures that define the nature of processing and lay down appropriate safeguards.

[54] Article 52 paragraph 1e, European Commission, European Parliament, *op. cit.* at note 5. This new obligation of supervisory authorities is influenced by relevant duty of the European Data Protection Supervisor under Regulation 45/2001 (Article 46e).

Data Protection Seal).[55] Their role is acknowledged also in the matter of approving *binding corporate rules*, *i.e.* personal data protection policies that are observed by EU controllers or processors for transfers of personal data to third countries in a group of corporate undertakings.[56] As regards *codes of conduct*, which are to contribute to appropriate application of the Regulation in particular across different industries *i.e.* data processing sectors[57], supervisory authorities' role in encouraging their drawing up is now explicitly introduced (in addition to initiatives of EU Member States and the European Commission) as well as their duty to provide opinions on draft codes submitted to them.[58]

The draft new rules on powers of supervisory authorities in many ways draw on, and build on solutions in the General Data Protection Directive, enumerating their powers in detail. These include *inter alia*[59] their authority to warn or admonish controllers or processors and order them to comply with data subject's requests under the Regulation, prohibiting data processing as well as transfers of data abroad to a third country or international organisation, ordering rectification, erasure or destruction of data processed contrary to the Regulation and ordering notification thereof to third parties (who received such data). For cases where the so-called *personal data breach* occurs[60], proposed entirely new power of supervisory authorities is ordering the controllers to notify affected data subjects on the breach.[61] *Investigative powers* such as accessing necessary personal data, documents and information are indispensable for efficient execution of supervisory authorities' tasks and these are included in draft Regulation in a way that generally follows related solutions in the General Data Protection Directive.[62] Additionally, right of access proposed in the draft Regulation extends also to all

---

[55] Article 52 paragraph 1(ja) and Article 53 paragraph 1(ia) in connection with Article 39 (additionally see explanations in recital 77), European Parliament, *op. cit.* at note 5. Certification would operate on a voluntary basis and it would be possible to have relevant audits carried out by third-party auditors on behalf of supervisory authorities. It is also proposed that the supervisory authorities may charge reasonable certification fees (taking into account administrative costs).

[56] Article 4 point 17; for details on binding corporate rules and relevant procedures see especially Articles 42-43 and 58, European Commission, European Parliament, *op. cit.* at note 5.

[57] Detailed provisions on codes of conduct are stipulated in Article 38 (additionally see recital 76), European Commission, European Parliament, *op. cit.* at note 5 (compare with Article 27 of the General Data Protection Directive).

[58] Compare Article 38 paragraph 2, European Commission, European Parliament, *op. cit.* at note 5.

[59] For a full list see Article 53, European Commission, European Parliament, *op. cit.* at note 5.

[60] Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Article 4 point 9, European Commission, European Parliament, *op. cit.* at note 5. For details on proposed data breach provisions see especially Articles 31-32, European Commission, European Parliament, *op. cit.* at note 5.

[61] Article 53 paragraph 1a, European Commission, European Parliament, *op. cit.* at note 5. Additionally see proposed Article 32 paragraph 4 (Communication of a personal data breach to the data subject).

[62] Article 53 paragraph 2a, European Commission, European Parliament, *op. cit.* at note 5 (compare with investigative powers according to Article 28 paragraph 3 of the General Data Protection Directive). It should be noted that according to amended draft text (European Parliament) the right of access would be granted *without prior notice* to the relevant controller or processor.

relevant premises.[63] Some restrictions may apply with respect to mentioned investigative powers.[64]

Introduction of *direct sanctioning powers* in the draft Regulation represents a paramount enhancement of supervisory authorities' powers in relation to the General Data Protection Directive.[65] I shall next examine key elements relating to this proposed new authority to sanction administrative offences, with a note that the Parliament's recent amendments introduced appreciable changes to original Commission's Proposal in that respect.[66] According to current draft text supervisory authorities could impose one or more sanctions, for *any non-compliance* with the Regulation, as follows. For first and non-intentional non-compliance, they could issue a *written warnin*g. Furthermore, they could order *regular periodic data protection audits*. Lastly a *monetary fine* can be imposed. This fine could amount to up to 100 000 000 Euro (100 million Euro) or 5% of the annual worldwide turnover in case of an enterprise, whichever is greater (where relevant controller or processor holds a valid European Data Protection Seal, it is proposed that the fine is not imposed unless a violation in question was intentional or negligent).

Sanctions must in each case be effective, proportionate and dissuasive and the criteria proposed to take into account when administering them include: nature, gravity and duration of non-compliance, whether non-compliance was intentional or negligent, degree of responsibility and previous breaches as well as repetitive nature of non-compliance, degree of co-operation with the supervisory authority to remedy infringement and mitigate possible adverse effects, personal data affected by infringement, level of damages suffered by data subjects as well as action taken to mitigate them, financial benefits or avoided loss from the infringement, refusal to co-operate with the supervisory authority or obstruction of its inspections, other aggravating or mitigating factors applicable to circumstance of the case, and internal compliance measures and programs undertaken by the relevant controller

---

63 Such power (right of access to premises) would according to amended draft text (Parliament) be granted *without prior notice* to relevant controllers or processors. EU law and law of respective Member State must be observed in execution of this authority. Article 53 paragraph 2b-last subparagraph, European Parliament, *op. cit.* at note 5 (additionally see explanations in recital 100).

64 With respect to investigative power of access, which would affect controllers or processors who are subject to a duty of professional secrecy, see draft Article 84 (European Commission, European Parliament, *op. cit.* at note 5) according to which Member States may adopt rules to ensure compliance with such duty of professional secrecy (or other equivalent duty of secrecy).

65 Article 79, European Commission, European Parliament, *op. cit.* at note 5.

66 With respect to monetary fines the Commission's Proposal envisaged three categories, for specified intentional or negligent violations of the Regulation, with the maximum fine amounting to up to 1 000 000 Euro (1 million) or 2 % of the annual worldwide turnover in case of an enterprise. This upper fine limit was significantly increased with the recently adopted amendments by the European Parliament (up to 100 000 000, *i.e.* 100 million Euro or 5% of the annual worldwide turnover in case of an enterprise, whichever is greater). For more details compare Article 79 according to original Commission's Proposal and according to amended text (Parliament), *op. cit.* at note 5.

or processor[67], *i.e.* degree of implementation of certain technical and organisational measures and procedures.

In further consideration of proposed sanctioning system and powers it is in my opinion also necessary to point to the subject of *consistency in enforcement*. Namely, according to current amended text of the Proposal (European Parliament) supervisory authorities would be obliged to co-operate with each other (also) in order to ensure a *harmonized level of sanctions EU-wide*.[68] This corresponds to proposed principal duty of ensuring consistency of application and enforcement of the Regulation.[69]

At the end of this analysis I would accentuate the pressing matter of *adequate resources* for the independent supervisory authorities, in order for them to be able to carry out their tasks and powers effectively according to draft Regulation. These authorities are already today experiencing difficulties in that respect in a number of Member States.[70] Unlike the General Data Protection Directive, draft Regulation clearly reflects on stated need in its operative provisions, *i.e.* article (as opposed to the recitals). In fact, it establishes a duty of Member States to ensure that these authorities are provided with *adequate human, technical and financial resources, premises and infrastructure necessary for effective performance of their duties and powers*, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board.[71] According to adopted amendments to the relevant recital (European Parliament), *population size and amount of personal data processing* are factors proposed to help determine adequate financial and personal resources for supervisory authorities.[72]

---

[67] See Article 79 paragraph (2c)(g) of amended draft text (European Parliament, *op. cit.* at note 5) in relation to proposed Article 23 (Data protection by design and by default), Article 30 (Security of processing), Article 33 (Data protection impact assessment), Article 33a (Data protection compliance review) and Article 35 (Designation of the data protection officer).

[68] Article 79 paragraph 1, 2nd sentence, European Parliament, *op. cit.* at note 5 (added 2nd sentence by the Parliament). Compare to explanations in proposed recital 120, European Commission, European Parliament, *op. cit.* at note 5.

[69] Article 52 paragraph 1c (see also explanations in recital 100), European Commission, European Parliament, *op. cit.* at note 5. Additionally see Article 46 paragraph 1, European Commission, European Parliament, *op. cit.* at note 5.

[70] European Union Agency for Fundamental Rights, *op. cit.* at note 24, in particular at p. 20.

[71] Article 47 paragraph 5, European Commission, European Parliament, *op. cit.* at note 5. As for the General Data Protection Directive, see explanations in recital 63.

[72] Recital 92, European Parliament, *op. cit.* at note 5 (newly added 2nd sentence). With respect to the issue of funding and adequate resources for supervisory authorities in light of the draft Regulation see also earlier proposals (2012) of the Article 29 Data Protection Working Party: „[…] Working Party strongly advises to more concretely indicate what amounts to an adequate budget, for example after an independent in-depth assessment of the increased costs for DPAs based on the current proposals has been carried out. An adequate budget could be based on a fixed amount to cover the basic functions that all DPAs have to undertake equally, supplemented by an amount based on a formula related to the population of a Member State and its GDP. There might also be an element to reflect the number of multinationals that have their headquarters established in that Member State. One of the recitals should explicitly encourage Member States to consider a variety of options for funding the DPA, so as to ensure it can meet the requirement of an adequately

3. Personal data protection law in Croatia: an overview

3.1. Introduction

The Republic of Croatia, the 28th and youngest European Union Member State that acceded to the European Union on July 1st 2013 has been aligning its legislative framework on personal data protection with the relevant *acquis* as of its application for EU membership. The Constitution of Republic of Croatia has already as of 1990 guaranteed the safety and secrecy of personal data as a separate constitutional right[73], however, it was only until 2003 that the first comprehensive act on general personal data protection was passed – *Croatian Personal Data Protection Act*.[74] On the basis of this act two decrees were adopted by the Government of the Republic of Croatia. The subject of one are methods of maintaining records on personal data filing systems and their form, and of the other, technical measures for the protection of special categories of personal data.[75]

The Personal Data Protection Act guarantees the right to personal data protection for all natural persons in Croatia, irrespective of their citizenship or place of residence and regardless of race, skin colour, sex, language, religion, political or other convictions, national or social background, property, birth, education, social standing or other characteristics.[76] As of its adoption up until today the Personal Data Protection Act has been amended several times and the amendments were also directed toward better alignment with the General Data Protection Directive. In fact, with the amendment in 2011 an article was explicitly introduced to declare alignment of the rules contained in this act with the General Data Protection Directive.[77] Apart from provisions of the General Data Protection Directive, the Personal Data Protection Act also contains main principles of Convention 108 and its Additional Protocol, which Croatia ratified in 2005.[78]

Rules regulating general personal data protection in Croatia apply to both manual and automated personal data processing and they apply to all relevant activities, both in the public and private sector. The only excluded area from their scope is the processing of personal data by natural persons solely for personal or

---

resourced authority." *Opinion 01/2012 on the data protection reform proposals*, 00530/12/EN, WP 191, 23.3.2012., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en. pdf, p. 17 (last accessed 20.10.2013).

73 Article 37 of the Constitution of the Republic of Croatia, Official Gazette of the Republic of Croatia no. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10 and 85/10 - consolidated text.

74 Personal Data Protection Act, Official Gazette of the Republic of Croatia no. 103/03, 118/06, 41/08, 130/11 and 106/12 - consolidated text.

75 Decree on the method of maintaining records on personal data filing systems and the form of such records, Official Gazette of the Republic of Croatia no. 105/04; Decree on the manner of storing and special measures of technical protection of special categories of personal data, Official Gazette of the Republic of Croatia no. 139/04.

76 Article 1 paragraph 3 of the Personal Data Protection Act.

77 Article 1a of the Personal Data Protection Act.

78 Official Gazette of the Republic of Croatia - International Agreements, no. 4/05 and no. 12/05.

household purposes.[79] However, legislative solutions providing for exclusion of application of the general personal data protection rules altogether also in certain other cases are not unknown.[80] The Personal Data Protection Act itself (as well as Convention 108 as ratified by Croatia) allows for derogations from application of certain data protection provisions, in specified circumstances.[81]

3.2. Personal Data Protection Agency

The Personal Data Protection Act established the national supervisory authority - *Croatian Personal Data Protection Agency* (further also as: Agency) with the core function of monitoring the processing of personal data in Croatia.[82] The Agency must perform its activities independently. It is responsible to the Parliament of the Republic of Croatia and funds for the Agency's operation are provided from the State Budget.

Any person who considers that any of his or her rights guaranteed by the Personal Data Protection Act were violated may submit a request to the Agency to establish a violation of rights[83]. This form may also be submitted electronically[84]. The Agency is authorized to temporarily ban the processing of relevant personal data (until finality of proceedings), should the person filing the complaint so require.[85] In addition to supervising implementation of personal data protection in Croatia, upon request of the data subject, proposal of a third party or on its own motion, tasks and activities of the Agency include: resolving requests to determine violations of rights guaranteed by the Act, drawing up a list of states and international organizations with adequate personal data protection regulation, co-operating with competent state bodies in preparing draft acts relating to personal data protection, monitoring regulation of personal data protection in other countries and co-operating with supervisory authorities in other countries, maintenance of

---

[79] Article 4 and Article 3 paragraph 4 of the Personal Data Protection Act, respectively. As for declarations of the Republic of Croatia with respect to Convention 108 (on the application of that Convention also to manual personal data files and non-application of this Convention to automated personal data files kept by natural persons solely for personal use or for household purposes), see: Council of Europe, *List of declarations made with respect to treaty No. 108*, available by search at: http://conventions.coe.int/, as well as the relevant ratifying act, Official Gazette of the Republic of Croatia – International Agreements no. 4/05. As for scope of application of the General Data Protection Directive, see its Article 3.

[80] For more details see Article 108 paragraph 4 in relation to Article 108 paragraph 3 of the Croatian Electronic Communications Act (Official Gazette of the Republic of Croatia no. 73/08, 90/11, 133/12 and 80/13), which excludes personal data protection rules from application as regards obligations imposed on operators towards the bodies authorized to apply secret surveillance measures (lawful interception of electronic communications networks and services).

[81] For more details see e.g. Article 23 in connection with Articles 9, 19 and 20 of the Personal Data Protection Act, Article 9 paragraph 2 in relation to Articles 5, 6 and 8 of Convention 108.

[82] Relevant provisions on the Agency and supervision of personal data processing in the Republic of Croatia are contained in Chapter IX of the Personal Data Protection Act (Articles 27-35).

[83] Article 24 of the Personal Data Protection Act.

[84] The submission form in Croatian is available at: http://www.azop.hr/cpage.aspx?page=contactRequest.aspx&PageID=55 (last accessed 20.10.2013).

[85] Article 25 of the Personal Data Protection Act.

the Central Register where records on personal data filing systems in Croatia are compiled, issuing proposals and recommendations for advancement of personal data protection, monitoring implementation of organizational and technical data protection measures, and proposing their improvement, monitoring transfers of personal data from Croatia. The Agency is also obliged to submit activity reports to the Parliament of the Republic of Croatia (annually at minimum) and these reports are public.

Powers of the Agency according to the Personal Data Protection Act include the issuing of warnings or notices on established irregularities, and these may be directed to controllers, data recipients as well as processors. The Agency may also issue decisions ordering that (any) established irregularity is resolved (eliminated) within a certain time period. It may also temporarily prohibit the processing of personal data in contravention of the Personal Data Protection Act. Furthermore, the Agency may order erasure of personal data collected without a legal basis, as well as prohibit unlawful transfers of personal data from the Republic of Croatia, or unlawful disclosures of personal data to data recipients. As to established violations with respect to data processing arrangements, the Agency may prohibit assignments of personal data processing tasks to processors in cases where the latter fail to fulfil applicable data protection requirements or where assignment of data processing tasks was (in general) conducted in contravention of the Personal Data Protection Act.

Decisions of the Agency noted above cannot be appealed to, however, administrative proceedings can be initiated against them before the competent (Administrative) court. The court practice is in this sense slowly developing in Croatia. According to the Agency's Activity Report for 2012, the Administrative court issued seven decisions on filed claims against decisions of the Agency, where it confirmed Agency's decisions in a total of six cases. During the period covered by the Activity Report there were a total of five claims filed before the Administrative court against decisions issued by the Agency.[86]

In addition to above stated measures and decisions, the Agency may also propose that criminal or misdemeanour proceedings are initiated at the competent authority, *i.e.* courts. It has no direct sanctioning authority.

The Personal Data Protection Act prescribes a single range of monetary fines that may be issued for violations of the Act (misdemeanours), amounting from a minimum of 20.000,00 to up to 40.000,00 Croatian Kuna (app. 2.625,00 – 5.250,00 Euro). Responsible persons in the legal person, state body and local and regional self-government bodies may also be fined, in the range from a minimum of 5.000,00 to 10.000,00 Croatian Kuna (app. 655.00,00 – 1.310,00 Euro). The fines have not been amended as of first adoption of the Data Protection Act in 2003 and they cannot be considered to be dissuasive in particular with respect to larger organizations. Furthermore, the Act itself prescribes no criteria for administering

[86] Personal Data Protection Agency, *Report on activities for 2012 – Izvjesce o radu za 2012. godinu*, June 2012, p. 24, http://www.azop.hr/download.aspx?f=dokumenti/Clanci/Izvjesce_o_radu_AZOP_za_2012.pdf (last accessed 20.10.2013).

the sanctions (e.g. maximum amount of fine that can be imposed according to severity of the violation, in case of repeated infringements, and other).

The above-mentioned monetary fine can generally be imposed in all cases where the controllers, data recipients or processors failed to abide by the Agency's orders of prohibitions. In other cases enumerated violations of the Personal Data Protection Act for which fines would be imposed are, as follows. Fines will be imposed on controllers who fail to respect the conditions stipulated in the Data Protection Act when disclosing personal data to data recipients for their use. Infringements of the rules on establishment, and keeping of records on personal data filing systems are also stipulated violations for which monetary sanctions can be imposed, as well as established violations of the controllers' duty to deliver records on personal data filing systems to the Agency in a prescribed deadline. Sanctions are also stipulated for cases where the controllers fail to notify the Agency on planned creation of personal data filing systems or of any further intended processing of such data.

Furthermore, violations of the duty to ensure adequate protection of personal data from accidental or deliberate abuse, destruction, loss, unauthorized alteration or access (required implementation of appropriate technical, personnel and organisational measures) are also explicitly envisaged breaches of the Act, for which a fine on controllers as well as data recipients can be imposed. Processors will also be sanctioned in cases of failure to implement the contractually stipulated measures of personal data protection. Fines would furthermore be imposed on processors where rules on assignment of personal data processing have been violated, in cases where they exceed their authority or process personal data for a purpose other than that agreed with the controller, or where they provide relevant personal data for use to other data recipients.

Failure on the part of controllers to respect the rights of data subjects that are guaranteed by the Personal Data Protection Act, consisting of a failure to complete, alter or delete their incomplete, inaccurate or outdated personal data, following such requests of the data subject, are also prescribed violations of this act for which a monetary fine can be imposed on them. Controllers can also be fined if they failed to appoint a data protection officer (appointment of data protection officers has become mandatory for controllers employing twenty or more employees as of amendment of the Personal Data Protection Act in 2011[87]). Additionally, the Act stipulates a monetary fine also for cases where the controllers, data recipients or processors prevent the Agency from conducting its tasks (*e.g.* where they prevent it from exercising its supervisory authority to access relevant information or where they fail to deliver documentation on request of the Agency, etc.). A monetary fine is also prescribed for violations of the Act by head of the Personal Data Protection Agency, deputy head and employees of the Agency's expert service, in cases of disclosure of confidential information that they came across in performance of their duties.

[87] For more details see Article 18a of the Personal Data Protection Act.

As mentioned earlier in this paper, the Agency may propose that criminal or misdemeanour proceedings are initiated at the competent authority, however, it has no direct sanctioning authority. According to the Activity Report for 2012 the Agency initiated in line with its powers a total of four misdemeanour proceedings as well as two criminal proceedings. [88] With respect to the latter it should be noted that the *Criminal Code of the Republic of Croatia* as currently in force prescribes *unauthorized use of personal data* as a criminal offense that is punishable by imprisonment from up to one to up to five years (depending on stipulated circumstances). Basic form of this criminal offense entails the acts of collecting, processing or using personal data in contravention of the law, which is punishable by imprisonment of up to one year.[89]

4. Concluding remarks

Proposed draft of the new EU general data protection legislation is one of the most - if not the most intensely lobbied act of European Union legislation[90], with almost four thousand amendments received, on which the European Parliament recently voted. Leaving aside the many proposed new duties of organizations processing personal data and reinforced accountability, such course of events with respect to draft new rules is in my opinion not too surprising in light of their extensive material and in particular territorial scope of application, *i.e.* wide international impact. In any case, negotiations on final text have been set to take place between the European Parliament, Council of the European Union and the European Commission. Consequently, current draft text of proposed Regulation may still undergo substantial changes before final adoption. While both the European Commission and the European Parliament expressed their wish to have negotiations concluded and thus the agreement finalized during the current term of the European Parliament in 2014[91], it remains to be seen if this really can be

---

[88] Personal Data Protection Agency, *op. cit.* at note 85, pp. 24-25.

[89] Article 146 of the Croatian Criminal Code, Official Gazette of the Republic of Croatia no. 125/11 and 144/12.

[90] Jan Phillip Albrecht - Rapporteur of the European Parliament for the Data Protection Regulation, *Lobbyism and the EU data protection reform*, http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/lobbyism-and-the-eu-data-protection-reform.html, 12.2.2013; Matt Warman, *Interview with Viviane Reding, Vice-President of the European Commission: EU Privacy regulations subject to 'unprecedented lobbying'*, „The Telegraph", http://www.telegraph.co.uk/technology /news/9070019/EU-Privacy-regulations -subject-to-unprecedented-lobbying.html, 08.2.2012 (last accessed 20.10.2013).

[91] Viviane Reding – Vice-President of the European Commission, *Women and the Web – Why Data Protection and Diversity belong together*, http://europa.eu/rapid/press-release_SPEECH-13-637_en.htm; SPEECH/13/637, European Commission Press Releases Database, 15.7.2013; European Parliament, *Q&A on EU data protection reform*, 22.10.2013, http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform (last accessed 25.10.2013).

accomplished. Following adoption of the Regulation it would take another two years (as of its entering into force) before it would apply in EU Member States.[92]

Should the final text of new EU rules be adopted as a regulation and should it contain rules at least similar to the ones examined in this paper, this will entail also significant consequences for the relevant national supervisory authorities. Comparative analysis of selected proposals of the new EU rules impacting supervisory authorities and related solutions in the General Data Protection Directive shows a serious reinforcement of powers attributed to these authorities, and an equally serious confirmation of crucial requirements for their independence in line with the case law of the Court of Justice of the European Union. At a more general level, the goals set to have a uniform set of rules and legal certainty, one-stop-shop mechanisms and equivalent level of protection of individuals' rights EU-wide clearly call for empowerment of data protection supervisory authorities throughout the EU as well as uniform duties, and the analyzed solutions impacting them in that respect should in any case be welcomed. In my opinion the need for empowerment of supervisory authorities may well arise already today, once the prescribed powers are considered comparatively in all European Union Member States. With that in mind I have also in this paper examined relevant legislation of the youngest EU Member State, Republic of Croatia, with adopted solutions on status, duties and powers of its national data protection supervisory authority in main focus. In my opinion these provisions declare marginal powers of the Croatian data protection authority, which in the overall negatively impact its vital role in the state's personal data protection system. Lack of this authority's direct sanctioning powers is troubling, currently especially in light of developments at the level of EU law that I analyzed in this paper. These observations are without prejudice to the fact that the General Data Protection Directive, which Croatia implemented, in many points does not provide for clear details on pertinent provisions, and leaves Member States ample discretion as to methods it would use to satisfy its rather basic requirements relating to supervisory authorities. Results of this are evident in studies and reports on implementation of the General Data Protection Directive in EU Member States, to which I referred to in the paper. I would here also draw attention to the issue of resources that the Member States would be obliged to ensure for the purpose of effective execution of tasks and powers of supervisory authorities according to draft Regulation. This I see as a potentially problematic issue on a broader level, especially taking into account possible limitations in state budgets and self-financing resources. For Croatia it is in any case important to already now consider the impact of draft Regulation on supervisory authorities and inquire into sources of possible funding and resources. Especially important in my opinion is work towards a more appropriate legal frame that can provide the Agency with direct sanctioning authority. Furthermore, work toward reconsideration of the present sanctioning system (misdemeanours and fines prescribed in the Personal Data Protection Act) would be desirable so as to

[92] Article 91, European Commission, European Parliament, *op. cit.* at note 5.

establish the criteria for administering sanctions and better reflect their dissuasive effect in justified cases.

Bibliography

1. András Jóri, *The End of Independent Data Protection Supervision in Hungary – A Case Study*, in: Serge Gutwirth;
2. Ronald Leenes; Paul De Hert, Yves Poullet (Eds.), *European Data Protection: Coming of Age*, Springer, 2013, pp. 395-406.
3. Article 29 Data Protection Working Party, *Opinion 01/2012 on the data protection reform proposals*, 00530/12/EN, WP 191, 23.3.2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion - recommendation/files/2012/wp191_en.pdf.
4. Douwe Korff, *EC study on implementation of data protection directive - Study Contract ETD/2001/B5-3001/A/49, Comparative summary of national laws*, University of Essex: Colchester – Cambridge, 2002, http://ec.europa.eu/justice/policies/privacy/docs/ lawreport/consultation/univessex-comparativestudy_en.pdf.
5. Douwe Korff, LRDP KANTOR Ltd (Leader) - Centre for Public Reform, *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*, 20.1.2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf.
6. Douwe Korff, *Data Protection Laws in the European Union*, The Direct Marketing Association - New York; Federation of European Direct Marketing Brussels, 2005.
7. 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, *Annex 2 Evaluation of the implementation of the Data Protection Directive*.
8. European Commission, *Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive*, COM(2007) 87 final, Brussels, 7.3.2007.
9. 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.
10. European Data Protection Supervisor, *EDPS pleading Commission v Hungary (C-288/12)*, 15.10.2013, https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/ Court.

11. European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Background documents and Compromise amendments (October 21, 2013 - meeting), *Compromise amendments 01 – 29; 30 – 91*, http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131021_1830.htm.
12. European Parliament, *Q&A on EU data protection reform*, 22.10.2013, http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform.
13. European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, 2010, http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf.
14. Jan Phillip Albrecht - Rapporteur of the European Parliament for the Data Protection Regulation, *Lobbyism and the EU data protection reform*, http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/lobbyism-and-the-eu-data-protection-reform.html, 12.2.2013.
15. LRDP KANTOR Ltd (Leader) - Centre for Public Reform, *Comparative study of different approaches to new privacy challenges, in particular in the light of technological developments, Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28, Final Report*, 20.1.2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/new _ privacy_challenges/final_report_en.pdf.
16. Matt Warman, *Interview with Viviane Reding, Vice-President of the European Commission: EU Privacy regulations subject to 'unprecedented lobbying'*, „The Telegraph“, http://www.telegraph.co.uk/technology/ news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html, 08.2.2012.
17. Personal Data Protection Agency, *Activity report for 2012*, June 2012, p. 24, http://www.azop.hr/download.aspx?f=dokumenti/Clanci/Izvjesce_o_radu_AZOP_za_2012.pdf (in Croatian).
18. Viviane Reding – Vice-President of the European Commission, *Women and the Web – Why Data Protection and Diversity belong together*, http://europa.eu/rapid/press-release_SPEECH-13-637_en.htm;SPEECH /13/637, European Commission Press Releases Database, 15.7.2013.
19. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, CETS No. 181, 08.11.2001.
20. Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 28.1.1981.
21. Council of Europe, *List of declarations made with respect to treaty No. 108*, http://conventions.coe.int/.
22. Charter of Fundamental Rights of the European Union, Official Journal of the European Union C 326, 26.10.2012.
23. 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.
24. Treaty on the Functioning of the European Union. Consolidated version of the Treaty on the Functioning of the European Union, Official Journal of the European Union C 326, 26.10.2012.
25. Regulation No 45/2001 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.

26. 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.
27. Constitution of the Republic of Croatia, Official Gazette of the Republic of Croatia no. 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10 and 85/10 - consolidated text (in Croatian).
28. Criminal Code, Official Gazette of the Republic of Croatia no. 125/11 and 144/12 (in Croatian).
29. Electronic Communications Act, Official Gazette of the Republic of Croatia no. 73/08, 90/11, 133/12 and 80/13 (in Croatian).
30. Personal Data Protection Act, Official Gazette of Republic of the Croatia no. 103/03, 118/06, 41/08, 130/11 and 106/12 – consolidated text (in Croatian).
31. Decree on the method of maintaining records on personal data filing systems and the form of such records, Official Gazette of the Republic of Croatia no. 105/04 (in Croatian).
32. Decree on the manner of storing and special measures of technical protection of special categories of personal data, Official Gazette of the Republic of Croatia no. 139/04 (in Croatian).
33. C-518/07 European Commission v Federal Republic of Germany, (2010) European Court Reports 2010 I-01885.
34. C-70/10 Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs (SABAM), (2011) European Court Reports, I-11959.
35. C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers (Sabam) v Netlog NV, (2012) European Court Reports.
36. C-614/10 European Commission v Republic of Austria, 16.10.2012 (not yet published - text of judgment is available at: http://curia.europa.eu).
37. C-288/12 European Commission v. Hungary, Official Journal of the European Union C 227, 28.07.2012, pp. 15-16.iut.