Conference of the International Journal of Arts & Sciences,
CD-ROM. ISSN: 1943-6114 :: 6(2):13–33 (2013)

THE COUNCIL OF EUROPE AND THE RIGHT TO PERSONAL DATA PROTECTION: EMBRACING POSTMODERNITY

Nina Gumzej

University of Zagreb Faculty of Law, Croatia

The author examines activities of the Council of Europe in regulating personal data protection, whose Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) is the first and to date only binding international legal instrument in this area. In particular, the author analyzes more recent activities towards a review of this convention and its Additional Protocol. Underlying reasons for the review as well as initiatives for global privacy and data protection standards are also discussed. Furthermore, the author studies the relationship of relevant developments in data protection at the level of Council of Europe with those at the level of European Union law, which is currently also in review. A separate section of this paper is devoted to an analysis of the draft proposal to revise (modernize) Convention 108 and its Additional Protocol according to text marked as final as of November 29th, 2012. In this analysis references are also made to proposed new rules at EU level and notably the EU Data Protection Regulation, towards a preliminary assessment of proposed solutions in the two frameworks and the level of consistency between them. The overall conclusion of this paper is that according to its draft revised Council of Europe convention incorporates admirable new and reinforced standards and mechanisms to ensure an effective system for safeguarding individuals' rights and freedoms, and especially their right to privacy, in postmodern data processing conditions, which facilitates data flows in today's globalized environment. Different approaches to implementation of general convention rules should not undermine required effectiveness of safeguards in practice, as this would undermine the very goals of this modernization and the degree of aspired harmonization internationally.

Keywords: Council of Europe, Convention 108, data protection, privacy, modernization

Introduction

These are exciting, dynamic times for data protection and privacy professionals worldwide. In fact, these are dynamic and exciting times for each and every one of us, as nowadays there is hardly an activity that does not, in one way or another entail the so-called "processing of our personal data". In European legal context these terms will mean a really large number of actions that can be done with a really large amount of data – our personal data. This is the data that relates to us as identified individuals, or as individuals who can be identified, whether directly or indirectly. Our personal data is being processed when any operation (or set of operations) is performed on them. In other words, processing takes place also when this data is collected, stored, disclosed, copied, erased, etc. In real life examples data processing takes place whether we are asked to provide our information directly, for instance to open up an email account, apply for a job, buy music or watch movies online, make a hotel reservation, apply for discount offers in shops. In many cases processing will be prescribed

by the law and will not require that we directly provide our data, as the data is already held somewhere and it is being processed according to that law and for the purposes prescribed by it. Alongside traditional, "offline" environment where the data processing takes place, we also opened up our presence in the digital, networked and globalized conditions. For example, whenever we connect to the Internet *i.e.* go "online" and use various online services that are being offered, data relating to us have presence in the digital environment that erases traditional territorial borders – the data often needs to be processed globally. With advance of technology, enormous sets of our digital data can be processed at great speeds and the many possibilities to put use into them are becoming more and more sophisticated and complex. It would not be an exaggeration to say that the postmodern data processing environment greatly increases also the scope of potential risks and challenges in relation to processing of our personal data, for us, our rights and our freedoms - and in particular for our right to privacy.

These dynamic and exciting times in privacy and data protection are particularly prompted by ongoing developments on modernization of rules, which govern this area at an international level. In my research I will examine relevant activities of the Council of Europe, which important international organization has a renowned background in regulating data protection and also aspires to set global standards in this field. Closely related to this are groundbreaking developments in data protection regulation at the level of European Union law, which I will also analyze in this paper. However, main focus of my research are activities towards a review of the Council of Europe *Convention for the protection of individuals with regard to automatic processing of personal data*, which was adopted in 1980 (further also as: "Convention 108"), and of its Additional Protocol [1]. Namely, Convention 108 is the first and until today the only binding international legal instrument in data protection. Forty-five countries ratified this convention until today. Latest accession by Uruguay also signifies the first accession to this convention by a non-European country [2] and furthermore, there are developments toward upcoming accession of Morocco, another country that is not a Council of Europe Member State [3]. The review referred to, or "modernization" of this convention, is motivated by the need to ensure the guarantees of human dignity and protection of human rights and fundamental freedoms, especially through *individuals' right to control their personal data,* in light of challenges that include in particular *diversification, intensification and globalization of data processing.* Moreover, *global promotion* of fundamental values of respect for privacy and personal data protection is a declared necessity, which supports *free data flows* [4].

Council of Europe Activities in Data Protection – Overview

It was already during the 70's that intensive work was carried out towards common international principles to ensure respect of individuals' rights and freedoms in the conditions of profuse automated processing of their personal data. Reaching agreement on a common set of principles was also a crucial objective for ensuring unrestricted, or at least easier international transfers of personal data. In this respect note must be made of relevant work of the Organization for Economic Co-operation and Development (OECD) and its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (further: "OECD Privacy Guidelines") that were adopted in 1980 [5]. These guidelines are not legally binding. Furthermore, work conducted in close connection with it at the level of Council of Europe resulted in almost parallel adoption of a *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Convention* (Convention 108). The convention is accompanied by the Explanatory Report with helpful, though non-authoritative interpretative assistance [6]. Due account of relevant work of OECD (OECD Privacy Guidelines) and the Council of Europe is evident in both instruments [7] and in fact, the

Convention 108 rule allowing accession also by non-Member States of the Council of Europe was drafted taking especially into account the non-European OECD countries [8].

Personal data transfers between Member States ratifying Convention 108 are enabled and operate under the main requirement of this convention, according to which all Parties to it must have in place adequate national laws. [9] Namely, each Party is obliged to incorporate into its domestic law the basic data protection principles of this convention, at the latest upon its entry into force with respect to that Party. This means that Convention 108 is not self-executing, *i.e.* directly applicable and the Parties must adopt measures in their domestic law that give effect to its relevant rules [10]. These are only minimum requirements and the Parties are free to provide for wider protection for data subjects in their domestic laws [11].

Basic data protection principles as set out in Chapter II of Convention 108 include the requirement to have personal data obtained and processed fairly and lawfully, stored for specified and legitimate purposes and not used in a way incompatible with those purposes. A stricter legal regime applies for automated processing of the more sensitive data ("special categories of data") [12]. Personal data must also be adequate, relevant and not excessive in relation to purposes for which they are stored, as well as accurate and kept up to date (where necessary). They also must not be kept in a form permitting identification of data subjects for longer than required for the purpose for which they are stored [13]. These rules will normally apply to the *controller of the file.* This is a person, public authority, agency or any other body competent under national law to decide on the *purpose* of automated data file, *categories of personal data* to be stored and on *operations* that are to be applied to them.

Furthermore, according to the *security safeguards principle* appropriate security measures must be applied so that personal data are protected against accidental or unauthorized destruction or accidental loss, unauthorized access, alteration or dissemination [14]. The data subjects must according to convention be enabled to exercise rights, which to a certain degree provide *them with control* over the collection and processing of their personal data. They must, for example, be able to establish if automated personal data files (with their personal data) exist and if so, establish their *main purpose* as well as identity of the controller. They also must be able to get a copy of their personal data (in intelligible form) and have their personal data rectified, or even erased in certain justified cases. The Parties are also obliged to provide for remedies in their national law, for cases where stated rights of data subjects and their requests have not been met [15]. It is important to note that the Parties are allowed to derogate from only a restricted set of basic data protection rules in the convention, and under prescribed conditions [16]. Furthermore, they must implement into their relevant national law appropriate sanctions and remedies for breaches of national rules giving effect to basic data protection principles of the convention [17].

The 2001 Additional Protocol on supervisory authorities and transborder flows (further: Additional Protocol) established important requirements on the function, authority and powers of (*data protection) supervisory authorities*, who are in charge of monitoring of, and ensuring compliance with relevant rules. A requirement for their independence is introduced, as well as that of the right of recourse to courts against decisions of these supervisory authorities. The Additional Protocol is important also for its rules on personal data transfers to states or organizations that are not Parties to Convention 108. This is in principle allowed, under the condition of ensured *adequate level of data protection* (with certain exceptions).

Council of Europe activities in data protection are not exclusive to its Convention 108 and Additional Protocol. Namely, in addition to the two early resolutions concerning *the protection of individuals vis-à-vis electronic data banks in the public and private sectors* (Resolutions (74) 29 and (73) 22), the Committee of Ministers of the Council of Europe has until today adopted a number of *recommendations* in the area. Their aim is to interpret and explain the application of general data protection principles of Convention 108 in a concrete environment, *i.e.* with respect to particulars of the different sectors and areas where data

processing takes place, and requires effective protection. Unlike Convention 108, these recommendations are not binding on Council of Europe Member States, however, the Committee of Ministers may request them to inform it on actions taken with respect to recommendations [18]. A "strong persuasive force" of recommendations was pointed to in legal doctrine [19]. In light of topic of this paper attention should in particular be given to the recommendations that address the specific challenges arising from development of advanced information-communications technology and data processing systems. For example, a recommendation adopted in 1995 addressed the challenges arising from the extensive increase of personal data generated with the use of telecommunication services as well as data stored by operators, in light of described technological development, and especially, digitalization of networks (*Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services*). This recommendation contains data protection principles based on Convention 108, as well as those deriving from guarantees to respect for private life and secrecy of communications pursuant to Article 8 of the European Convention on Human Rights (further also as: "ECHR"). By way of example, the recommendation includes specific safeguards to ensure confidentiality of communications and security requirements vis-à-vis networks and services, transparency requirements as regards data processing, the principle of minimizing personal data collected when using telecommunication services and the purpose limitation principle as regards processing relevant data. The principle to have networks, equipment and software designed and operated in a privacy-compliant way is also included in this recommendation, as well as many other guarantees of users' rights (*e.g.* in relation to subscriber directory inclusion and use of personal data for direct marketing purposes, calling-line identification, itemized bills, call-forwarding, anonymous access to networks and services, and other). As of 1995 when this recommendation was adopted specifically for the telecommunications sector, further technological development and especially increased use of the Internet and various online services led to advanced proliferation of personal data processing and the more sophisticated data processing technologies and systems. Therefore, activities at the level of Council of Europe focused more on addressing the modern challenges of pervasive personal data processing in the online environment for rights and freedoms of individuals, and in particular their right to privacy. Accordingly, the latest recommendations adopted by the Committee of Ministers address the specific area of profiling, and the online search engines and social networking services. The table below shows which recommendations it has adopted according to what sectors and areas until today, in chronological order:

RECOMMENDATIONS OF THE COUNCIL OF EUROPE COMMITTEE OF MINISTERS IN THE AREA OF DATA PROTECTION (as of April 5th, 2013) [20]
Recommendation No.R(81) 1 on regulations for automated medical data banks (23 January 1981) [replaced by Recommendation No. R (97)5]
Recommendation No.R(83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983) [replaced by Recommendation No. R(97) 18 with regard to statistics]
Recommendation No.R(85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985)
Recommendation No.R(86) 1 on the protection of personal data for social security purposes (23 January 1986)
Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987)
Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (18 January 1989)
Recommendation No.R(90) 19 on the protection of personal data used for payment and other operations (13 September 1990)
Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991)
Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995)
Recommendation No.R(97) 5 on the protection of medical data (13 February 1997)
Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997)

Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999)
Recommendation No.R(2002) 9 on the protection of personal data collected and processed for insurance purposes (18 September 2002)
Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010)
Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines
Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services

Towards Postmodern Global Standards?

The Council of Europe significantly contributes active global harmonization in the area of personal data protection. A *Data Protection Day* is commemorated in Europe as of 2007 each year on the date the Convention 108 was opened for signature (January 28th, 1981) [21], which is today celebrated also outside Europe, including the USA and Canada under the name *Data Privacy Day* [22]. Global appeals in particular in the scope of *International Conferences of Data Protection and Privacy Commissioners* have long been made towards a proactive role of the Council of Europe, *i.e.* to invite not-Member States of the Council of Europe, with relevant laws, to accede to the Convention and its Additional Protocol. Countries world-wide are urged to ratify these instruments [23]. Accordingly, the Council of Europe has especially in the past years actively promoted benefits of global accession to Convention 108 [24] and as explained earlier, Uruguay was the first non-European country to accede in 2013 and it is expected Morocco will follow as another country that is not a Council of Europe Member State. Promoted accession to Convention 108 and its Additional Protocol globally should be looked at also in light of initiatives and work carried out to review its rules, in a way that would allow it to claim a (potentially universal/ global) standard-setting character and role. This relates to considerations on the need to adapt data protection principles to the post-modern data processing context. Newer challenges for rights and freedoms of individuals with respect to processing of their personal data, and especially their right to privacy are denoted in particular by the rapid development of more advanced information-communication technologies, systems and services and accentuated by trends in globalization. The post-modern social context towards the need for global privacy and data protection standards must not here be disregarded, especially in light of increased surveillance measures supported by the use of sophisticated surveillance/data processing technologies and systems. This is often accompanied by a function creep in data protection terms, *i.e.* use of personal data for such purposes although the data may originally have been collected from a data subject to be processed further only for a private, *e.g.* commercial purpose. Generally speaking mass surveillance measures are at a global level intended for the purpose of fighting serious crime, and in particular terrorism.

All described developments prompted especially in the scope of mentioned International Conferences of Data Protection and Privacy Commissioners, calls for a *globally enforceable set of rules on personal data and privacy protection* as well as a new international privacy protection framework, founded on rule of law and respect for human rights, as well as the support for democratic institutions[25]. Drafted international privacy and data protection standards represent a notable result of all these initiatives [26]. Calls were also made to the *United Nations* (UN), to create a binding instrument where personal data protection and privacy rights would be established as enforceable human rights, clearly and in detail [27]. In that respect it is important to note a report of the *Special UN_Rapporteur on the promotion and protection of human rights while countering terrorism* [28]. The reason for this are numerous recommendations issued to the states as well as the UN Human Rights Council, on measures that are necessary to ensure stronger enforcement of the right to protection of

privacy, including the right to personal data protection in the mentioned context of fight against terrorism. According to the report, personal data protection in light of development of information technologies, which enables the previously inconceivable functionalities with respect to personal data processing, is not only interpreted as part of the right to privacy protection (*International Covenant*) [29], but it is furthermore becoming a separate fundamental human right. The fact that a number of countries today already afford data protection the status of a separate constitutional right, accentuates its importance as an element of democratic society. The Special Rapporteur also urged the UN Human Rights Council to establish a process building on existing data protection principles to recommend measures for constituting a *global declaration on data protection and data privacy* [30].

While a comprehensive analysis of all globally available instruments as well as methodology towards international harmonization of privacy and data protection goes beyond the scope of this paper [31], when considering prospects of a new UN Treaty on this topic I would agree with those commentators who consider low prospects for adoption of such universal treaty, especially in any nearer future [32]. On the other hand, Convention 108 as a binding international legal instrument that is already in force has a solid starting point to reach if not globally, then at least predominantly international legal harmonization in this area [33]. For example, Greenleaf, considers it as „the only realistic possibility for a global binding international agreement on data protection to emerge"[34], or „at least as promising a candidate for globalization as the Cybercrime Convention. Despite this theoretical possibility, there is as yet little of substance to suggest that Convention 108 will become a key instrument of global governance of privacy, despite its great potential to do so. However, it has no realistic competitors as a global privacy instrument"[35].

Acknowledging the fact that Convention 108 with its Additional Protocol has until today remained the only binding international instrument in the area of personal data protection, with a growing influence on data protection laws also outside Europe, and taking into account the possibility for accession also by countries that are not member states of the Council of Europe, it can indeed be considered a legal instrument with a potentially world-wide application. In this paper I have shown a clear necessity for such rules in the today's post-modern heavily globalized world. However, in addition to the need to actively support and promote accession by as many countries with relevant laws [36], the Convention 108 together with its Additional Protocol itself requires a revision to better address the earlier described challenges of the post-modern era and society, which are in particular denoted by pervasive data processing in light of progressive technological developments. This was recognized at the Council of Europe [37]. Following an extensive report into areas of possible revision [38], the Council of Europe organized public consultations at the occasion of the 30th anniversary of Convention 108, which, understandably, prompted many responses from interested parties world-wide [39]. Further work in the area resulted in the draft final proposal of revised Convention 108 and Additional Protocol, with an accompanying draft explanatory report, which I will examine in section V of this paper.

Prior to that analysis, in next section of this paper I will provide an overview of key developments in the regulation of personal data protection at the level of European Union law, and examine their connection with relevant Council of Europe developments. I will focus on the EU general personal data protection rules, which are also currently in review, especially taking into account the close connection with the Council of Europe framework and requirements of consistency between the two frameworks. This is, however, without prejudice to all other relevant binding and non-binding legal-regulatory frameworks and related developments internationally, which are also considered in the process of reviewing Convention 108 and its Additional Protocol. These include *inter alia* the earlier mentioned International Standards on the Protection of Privacy with regard to the processing of Personal Data (as welcomed at the 31st International Conference of Data Protection and Privacy

Commissioners – the Madrid resolution), regional *Asia Pacific Economic Cooperation Privacy (APEC) Framework*), and other [40]. It is important to have in mind, especially taking into account a close connection between the Council of Europe and the OECD on drafting international data protection and privacy principles, as explained in previous section that, aside from ongoing efforts towards modernization of Convention 108, currently in process is also a review of the OECD Privacy Guidelines [41]. This work was, of course, also considered in review of the Council of Europe convention.

Relevant Developments in European Union Law

The possibility for accession of the European Union to Convention 108 was enabled by its amendment in 1999 [42], and recently the European Commission announced a recommendation, which enables it to negotiate its review on EU's behalf. It also expressed the intention to have EU's "gold standard of data protection" accounted for in this review, *i.e.* modernized convention [43]. The main EU data protection instrument, *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* (further: "General Data Protection Directive") [44] is in fact considered in the doctrine as „leading trendsetter and benchmark for data protection around the world" [45] and „most significant overall influence on the content of data privacy laws outside Europe" [46]. Its influence was predicted to increase in non-European countries (data protection laws) also due to their motivation to be recognized as countries with *adequate levels of data protection* (which enables or significantly simplifies personal data transfers under the applicable EU legal regime) [47]. In general terms the General Data Protection Directive allows personal data to be transferred to such third countries if they ensure adequate levels of data protection, which is decided by the European Commission [48]. This directive applies to all EU Member States and to Norway, Iceland and Lichtenstein as Member States of the European Economic Area (EEA) [49]. It was passed in 1995 with the intention to ensure EU-wide protection of rights and freedoms of natural persons, and most notably their privacy rights, with respect to processing of their personal data. The intention was also to ensure conditions for further development of the EU's internal market by unrestricted data transfers, primarily taking place between the EU/EEA Member States implementing the directive into their national law. This directive has a general scope of application, which means that it applies to any processing of personal data, regardless of technology used or type of processing [50]. The directive reflects great influence of relevant international law sources of the Council of Europe, notably the ECHR, and the data protection and privacy principles of the directive are proclaimed to *give substance to and amplify those contained in Convention 108* [51]. Likewise, the rules adopted in the 2001 Additional Protocol to Convention 108 and to which I pointed earlier in this paper, share certain core data protection requirements of the General Data Protection Directive, as regards supervisory authorities and transborder personal data flows.

It is important to here also make note of the later adopted sectoral directive, which regulates personal data processing and privacy protection in telecommunications, and which builds on the General Data Protection Directive [52]. Similarly as in the earlier pointed to Recommendation (No.R(95) 4) of the Council of Europe Committee of Ministers, special regulation of this area was also at EU level prompted by digital technology developments in public communication networks and related considerations of new challenges for privacy and personal data protection rights. It was also necessary to create the conditions for raising trust of users, while promoting further development of telecommunications services and networks, as well as the information society in the EU's internal market [53]. The rules contained in this directive show similarity with data and privacy protection principles in the mentioned

Council of Europe recommendation. Subsequently this directive was amended by Directive 2002/58/EC (further: "Directive on privacy and electronic communications") that is currently in force [54]. Considerably higher data processing capacities and possibilities of new digital networks, and especially development of the Internet are further catalysts for regulation of this specific area [55].

Over the last years recognition of personal data protection law significantly evolved in EU law. Today the right to personal data protection is guaranteed pursuant to Article 8 of the binding Charter of Fundamental Rights of the European Union [56], separately from the otherwise very closely related right to respect of private life and communications [57]. Furthermore, the right to personal data protection is guaranteed to everyone pursuant to Article 16 of the Treaty on the Functioning of the European Union [58]. According to the relevant new procedure and legal basis a new EU data protection framework is currently in legislative procedure [59]. It includes also the proposed *General Data Protection Regulation*, which is to repeal the General Data Protection Directive [60]. It is expected that the legislative procedure on this regulation would be completed sometime during 2014 and that the new rules would apply (according to the transition period in draft proposal) two years as of its entering into force, *i.e.* during 2016 [61]. I will here point to four elements of the proposed regulation, which should especially be taken into account in assessment of the topic of this paper. Firstly, the new rules are intended toward better adaptation of personal data protection law and especially enforcement thereof, in the overall context of the post-modern digital age that is largely technology-driven. As such the new rules aim to consistently cover also the data processing activities in the online, networked digital environment. Secondly, the rules are proposed to be adopted in the form of an EU regulation. Such legal instruments, unlike the EU directives, apply directly and entirely in all EU Member States [62]. Next, according to proposed scope of application the new rules would cover also organizations that are not established in the EU. This is when their data processing activities relate to the offering of goods or services to EU residents, or to the monitoring of their behavior (*e.g.* where a non-EU controller tracks the behavior of EU residents on the Internet for profiling purposes) [63]. Finally, a number of rules proposed aim to ensure stronger protection of data subjects and accordingly, stricter and legally enforceable accountability of those who are in charge of processing personal data. This will not only entail obligations to implement various policies and measures for *ensuring compliance* of relevant data processing operations with new rules, but also *demonstrating such compliance*, primarily to the relevant data protection supervisory authority [64].

Work on modernization of Convention 108 and its Additional Protocol closely follows mentioned revision of the EU data protection framework. Obviously, intention is to ensure their compatibility and coherence [65]. This is a goal historically pursued also with respect to the EU General Data Protection Directive (which is currently still in force). Intended consistency of relevant legal frameworks may, on the other hand, require more adjustment in timing. Namely, proposed new EU data protection framework is currently undergoing extensive discussions in the context of relevant legislative procedure, which may result in (many) amendments to the originally proposed rules by the European Commission. On the other hand, work on revision of Convention 108 and its Additional Protocol appears to have reached a final phase [66]. In next section of the paper I will examine selected highlights of the draft proposal to revise the convention, according to text marked as final as of November 29th, 2012 (further also as: "Proposal") [67]. Where relevant I will also analyze the Proposal according to text of the draft explanatory report (further also as: "Draft Explanatory Report" or "draft report") [68]. While this text may facilitate application of the Proposal, this is without prejudice to the earlier explained non-binding character of explanatory reports, *i.e.* non-authoritative nature of relevant interpretations that they contain [69].

Draft Revised Convention 108 – Overview

According to the Proposal, intention of revised convention is to ensure that personal data of all natural persons, who are *subject to jurisdiction of the Parties* (whatever their nationality or residence), are protected *when processed*, which contributes to the respect for their rights and freedoms and especially their right to privacy. As further clarified in the Draft Explanatory Report, the right to protection of personal data is not an isolated but an *enabling right*, without which other rights and freedoms "could not be exercised and enjoyed in the same manner" [70]. This is supported by relevant case law of the European Court of Human Rights, according to which data protection is of fundamental importance to the enjoyment of individual's right to respect for private and family life, which is guaranteed by the ECHR [71]. The report also acknowledges the status of personal data protection under European Union law as a separately guaranteed fundamental right, which was pointed to earlier in this paper. Personal data protection is not, however, an absolute right. It needs to be considered in respect of its role in society and reconciled with other rights and freedoms [72].

The revised rules are proposed to have a *wider scope of application* than the current Convention 108. This is already visible from the amended title (*Convention for the Protection of Individuals with Regard to the Processing of Personal Data*), which replaces the current term "automatic processing" with "processing". Accordingly, the new concept of *data processing* will be introduced, replacing the current concept of "automated processing". It is important to have in mind that the new data processing concept would be broader. It is intended to cover any operation or set of operations performed upon personal data, and in particular collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data. In addition to processing by automatic means, data processing will include also manual processing, which denotes „operations carried out within a structured set established according to any criteria which allow to search for personal data" [73]. By meaning this concept is aligned with the EU General Data Protection Directive, as well as the proposed General Data Protection Regulation [74].

As regards revised convention's scope of application, it will according to the Proposal apply to all processing of personal data (in both the private and public sectors). During work on the Proposal, such scope of application that enables effective protection "against privacy intrusions by public and private authorities, both in the offline and on-line worlds" was commented as cross-cutting [75]. The exception to this is processing of personal data by natural persons in order to carry out purely personal or household activities, which is now explicitly envisaged in text of revised convention [76]. The two instruments are aligned as to the exception of personal or household activities, with a little support from the Draft Explanatory Report, according to which such processing will have no professional or commercial grounds (no gainful interest) [77]. Generally the scope of revised convention would be wider in comparison to that of the proposed General Data Protection Regulation (although this mainly results from the distribution of competencies between the EU and Member States, and the fact that certain areas are regulated by other EU instruments) [78]. Such wide scope is, however, without prejudice to the possibility of the Parties, to derogate from some of the basic data protection principles of revised convention, under strictly prescribed conditions and in specified cases (they must prescribe the derogation by law, which must be a necessary measure in democratic society for the protection of national security, public safety, important economic and financial interests of the State or the prevention and suppression of criminal offences; or for the protection of data subjects or rights and freedoms of others, especially freedom of expression), or to lay down restrictions under certain conditions and in specified cases [79].

In accordance with the current rule in Convention 108, which I explained earlier in the paper, the Parties are free to prescribe a wider scope of protection (than according to the revised convention) for data subjects, in their domestic law [80].

In addition to the need to modernize convention rules to better address the earlier described needs and challenges, it is also necessary to ensure *stronger* a*pplication* and *enforcement* of data protection principles by all Parties. New provisions are therefore added to *ensure application* of the revised convention and *effective monitoring of required compliance* by the Parties. Currently the Parties must adopt measures giving effect only to the basic data protection principles (as set out in Chapter II of Convention 108) and at the latest at the time of its entry into force with respect of that Party. According to the Proposal, however, the Parties will be obliged to implement the entire (revised) convention, and at the latest until ratification or accession [81]. Furthermore, specific monitoring mechanisms are introduced to ensure that the Parties effectively apply the revised convention, as implemented in their national law. The *Convention Committee* will have a role to that effect, which is to replace the current Consultative Committee and assume stronger powers. It would *inter alia* prepare opinions on candidates' levels of data protection to accede to the revised convention (for the Committee of Ministers) and also periodically monitor implementation of the revised convention by the Parties. The Parties will also be obliged to *actively contribute* to such monitoring ("evaluation") of their obligations [82]. Stronger powers and functions of relevant *national supervisory authorities* (data protection authorities) and a *reinforced mutual co-operation* is vital for achieving all mentioned objectives, and for achieving aims of the revised convention in general. Consequently, the Proposal builds on relevant provisions of the Additional Protocol by advancing their independence, stronger role and specifying powers, tasks and functions. It would be mandatory for the Parties to also ensure that supervisory authorities have adequate resources for exercising their powers and functions independently and effectively. The Proposal further clarifies the essential requirement of their independence, and adds weight to ensure more effective co-operation between the Parties, *i.e.* their supervisory authorities [83]. Solutions towards, *inter alia*, reinforcement of powers and ensured independence of data protection authorities as well as stronger and more effective mutual cooperation mechanisms are all reflected in the proposed General Data Protection Regulation [84], which also further develops on current solutions in the General Data Protection Directive and integrates relevant case law (EU *acquis*), where applicable [85].

With respect to cross-border data transfers the Proposal marks changes to the current regime in the manner expected. I will here focus only on selected changes that I find critical [86]. The main principle allowing for cross-border data transfers remains the same - there must be ensured *appropriate level of data protection* (currently referred to as adequate level of protection for intended data transfer in the Additional Protocol). This would enable in principle unrestricted data transfers between the Parties to revised convention (appropriate level is presumed for them). Exceptions to this would be cases where the exporting Party is regulated by *regional binding harmonized rules* and where data transfers are *not governed by ad hoc or approved standardized safeguards* (*e.g.* contractual clauses) that must be *legally binding, enforceable and implemented* by persons involved in the transfer and further processing of relevant data. For data transfers to non-Parties, the criterion of appropriate level of data protection is proposed to be ensured not only by their laws, *but also by earlier mentioned safeguards*. In relation to the EU framework in my opinion the proposed changes aim towards ensuring consistency for cases where, for example, the recipient Party presumed to have appropriate data protection levels under the revised convention is not at the same time recognized under the EU framework (to ensure adequate level of data protection). The Proposal attaches significant weight to the above-mentioned *ad hoc* or approved standardized safeguards, as *additional safeguards* for enabling cross-border data flows. This is in line with relevant developments under the proposed General Data Protection Regulation [87]. For these

reasons I would consider harmonization of requirements for approving relevant safeguards (under the EU framework and the revised convention) as highly necessary [88].

Certain basic data protection concepts that were re-drafted or newly added into the Proposal are explained "to cover, where necessary, different terms or concepts used in national legislation to express certain fundamental concepts" [89]. In the overall it can be said the concepts correspond to terminology of the General Data Protection Directive, such as the concept of a *data controller* (which is to replace "controller of the file") and the newly introduced terms of the *recipient* (of personal data) and *data processor* [90]. As regards the meaning of key concept of *personal data*, the Proposal does not amend it. In other words, personal data continue to mean any information relating to identified or identifiable individual, *i.e.* data subject. However, the Draft Explanatory Report provides further guidance that is necessary on this critical but often complex issue and as expected, it also acknowledges importance of the issue of identification in the online environment. Thus according to the report identification can be done by referring to a certain person or to an access point or device (*e.g.* terminal equipment such as a personal computer, mobile phone, etc). It also clarifies that the criterion to establish if a person can be identified or not, does not only concern his or her civil identity (*e.g.* name, surname), but also those identifiers that allow to *single a person out* or distinguish it from others (*e.g.* IP addresses as digital identifiers, as well as physical, physiological, genetic, mental, economic, cultural or social features of a person). A person is not to be considered identifiable if such identification requires unreasonable time or effort for the data controller, *or for any other person from whom the controller could reasonably and legally obtain the identification* [91]. On the whole explanations here provided do seem to take account of the relevant EU *acquis* [92] and at minimum some of the main directions on the issue under the proposed General Data Protection Regulation [93], including its recitals [94]. The Proposal also introduces requirements for data subject's *consent*. Consent is one of the two main grounds for lawful processing of personal data (the other is a legitimate basis, which is laid down by the law). It specifies that such consent of the data subject must be *specific, informed and explicit/unambiguous* [95]. Additional text in the Draft Explanatory Report especially suggests similarity of this data protection concept with that in the proposed General Data Protection Regulation [96].

In addition to adjustments required in order to consistently apply the new concept of data processing, to which I pointed previously, the Proposal redesigns and reinforces certain key principles of Convention 108. An important new rule on *proportionality of data processing* aims to ensure that the processing is proportionate to the legitimate purpose pursued, and that it reflects *at all stages* a fair balance between all (public or private) interests concerned, and the rights and freedoms at stake. According to the Draft Explanatory Report, this includes the requirement to ensure that the data processing is *necessary*. This would mean that there are no other appropriate and less intrusive measures with respect to interests concerned, and rights and freedoms of data subjects [97]. Furthermore, personal data must according to redesigned *data minimization* principle not only be adequate, relevant and not excessive in relation to processing purposes, but they also must be *limited to the minimum necessary in relation to these purposes* [98].

Building on current solutions in Convention 108, the draft revised convention is to ensure a *clear transparency duty of the data controller* towards data subjects as regards processing of their personal data [99]. The Parties can derogate from this obligation under certain conditions [100]. As a rule (subject to certain exceptions), information that must be provided to data subjects include at least the information on identity and habitual residence or establishment of the controller, processing purpose(s), personal data processed, recipients or categories of recipients, means of exercising data subjects' rights, as well as any other information necessary to ensure fair and lawful data processing. These information

requirements, especially when read together with the Draft Explanatory Report, closely relate to those proposed in the General Data Protection Regulation [101].

In addition to current "additional safeguards" for data subjects according to (Article 8 of) Convention 108, such as the right to have their personal data rectified, or erased if processed contrary to the law, the Proposal advances certain safeguards for data subjects that are now strengthened, as well as rights (entitlements) that are altogether new. It needs to be noted at the outset that the Parties would be allowed to derogate from these obligations in prescribed cases [102]. Although the list of rights in the draft new Article 8 is longer, I will here only point to a few selected examples. *Extended information requirement* towards data subjects is an example of a strengthened right of data subjects. In other words, data subjects would be entitled to get on request also all available information on the origin and retention period of their personal data, as well as any other information that the controller must provide to fulfill the transparency duty (as examined above). Example of a *new* right granted to data subjects is the *right to object* at any time to (any) processing of their personal data, unless the controller demonstrates compelling legitimate grounds for processing, which override their interests or rights and fundamental freedoms. While such right to object may seem very extensive, the draft Explanatory Report helps to clarify that it always needs to be reconciled with other rights and legitimate interests [103]. The right to *obtain, on request, knowledge of the reasoning underlying the data processing* (the results of which are applied to data subjects) is also new. The same goes for the right *not to be subject to a decision significantly affecting the data subject, which is entirely based on automatic processing without having data subject's views taken into consideration*. In this respect note must be made also of the recommendation on profiling that was adopted by the Council of Europe Committee of Ministers in 2010, to which I referred in section 2 of this paper [104]. A quick comparison of this draft with the relevant EU framework shows similarity with the rules that are currently in force under the General Data Protection Directive, and where this is not the case there is some similarity with the more progressive solutions in the proposed General Data Protection Regulation [105]. The Draft Explanatory Report is shy on comments and additional details on these important (and general) rules on data subjects' rights. Hopefully more progress can be achieved in that respect.

With respect to special categories of data that are to become *sensitive data* under the Proposal, stricter legal regime for their processing would extend to *genetic data*, and to the *biometric data that uniquely identifies a person*. Additionally, it would also apply to processing of personal data that not only concern (as currently under Convention 108) criminal convictions but also offences as well as related security measures. As clarified in the Draft Explanatory Report, such data are to be considered sensitive by their very nature. In this sense a distinction is made with the data that need not by nature (always) be sensitive, but that become sensitive when processed (according to purpose of the processing). This applies to the processing of personal data *for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life*. All such processing is just as today under Convention 108 only to be allowed if the relevant law prescribes appropriate safeguards. However, an important new provision adds a clarification on the function of such *appropriate safeguards*. These safeguards need to ensure prevention of risks, which the processing of sensitive data may entail for interests, rights and fundamental freedoms of the data subject, and in particular the risk of *discrimination* [106].

The draft revised convention introduces a duty of data controllers to report *serious personal data breaches* to the relevant (data protection) supervisory authority. Such reporting must be done without delay. Only those data breaches that occurred must be reported, *which may seriously interfere with rights and fundamental freedoms of data subjects* [107]. It is also envisaged that the Parties may derogate from this duty, in strictly prescribed cases [108]. According to the Draft Explanatory Report, examples are breaches resulting in significant

risk of financial, reputational, physical harm or humiliation to the data subject. Data breach rules will also form part of the future EU general data protection framework [109], as inspired by the already applicable data breach rules in the electronic communications sector, according to the earlier mentioned Directive on Privacy and Electronic Communications [110]. Namely, the controllers would be obliged to notify all breaches to the data protection supervisory authorities according to proposed General Data Protection Regulation. Additionally, they would in certain cases also be required to communicate them to data subjects. A quick comparison of the two draft frameworks shows that the Proposal limits the duty to notify breaches to supervisory authorities only for serious breaches as explained above. Furthermore, it does not introduce mandatory notifications of data breaches also to data subjects (for special cases). On the other hand, additional details provided in the draft report point to a degree closer to the proposed measures in the General Data Protection Regulation (as a type of best-practice recommended approach) [111].

In conclusion of this overview I will summarize a set of new rules in the draft revised convention, which are titled as *additional obligations* [112]. In my opinion these obligations are crucial to the goals of attaining an effective data protection framework in postmodern data processing conditions, as laid out in the Proposal. These new rules are based on the principle of *reinforced accountability* of those who are in charge of processing personal data. In essence it means that in addition to measures and policies that the responsible persons/entities must implement to *ensure compliance* with data protection rules, they also need to be able to *check such compliance* as well as put in place measures enabling them to *demonstrate* it, notably to the (data protection) supervisory authorities. In this respect I would also draw attention to proposed extension of relevant data protection duties to the data processor, as a person/entity that processes personal data on behalf of the controller. Namely, earlier in this paper I explained that the Proposal would introduce for the first time the concept of a data processor in the revised convention. One example of extended application of data protection obligations to data processors is the duty to apply appropriate security measures against accidental or unauthorized access, destruction, loss modification or dissemination of personal data. [113]. This requirement is, in comparison to the relevant EU framework, already envisaged in the General Data Protection Directive [114]. The proposed General Data Protection Regulation further extends the scope of data protection obligations to processors (where applicable) [115]. That is in line with requirements for reinforced accountability in data protection, which are demonstrated in many of its provisions [116]. As I will show next, this necessity and trend is closely followed in the Proposal.

Additional obligations in the Proposal entail in the first place a duty of all Parties to provide that the controller, *or where applicable the processor*, must take at *all stages of processing all appropriate measures* to: a) *implement* the rules giving effect to principles and obligations of the revised convention; b**)** *establish internal mechanisms to verify compliance* with relevant rules and to be able to *demonstrate such compliance* (at least to the supervisory authority) [117]. Furthermore, the Parties must provide that controller, *or where applicable the processor*, carries out *analysis of risks* that the intended data processing may have for rights and freedoms of data subjects (*data protection impact assessment* under the proposed General Data Protection Regulation) [118] and moreover, that the processing operations are *designed* so that any such risk is prevented or at least minimized. This important duty to apply *privacy by design* (*data protection by design* and *by default* under the proposed General Data Protection Regulation) [119] especially entails a requirement that implications of the data protection right are taken into account *as early as from the stage of designing products and services for data processing*. Additionally, such products and services are to *facilitate compliance* of data processing with the applicable law.

These new obligations are not intended to apply as one-size-fits-all rules. In other words, the Parties would be able to adapt application of these rules in relation to the size of the data controller, volume or nature of processed data, and in light of risks involved for data subjects.

The Draft Explanatory Report expressly refers to a high similarity of these new rules, with the requirements established under the APEC Privacy Framework and its Cross-Border Privacy Rules [120]. Again it is the details laid out in this report, which help to clarify the (possible) steps and measures towards implementation of the new additional obligations in practice [121]. Implemented measures and policies to that effect must in any case be strong, effective and applied continually (maintaining compliance is a process). In comparison to the EU framework, as already indicated above these additional obligations show good correlation with relevant key rules of the proposed General Data Protection Regulation (which are, understandably, much more detailed). This is supported by details in the draft report, which, for example, suggests measures such as appointment of data protection officers [122] and implementation of easy-to-use mechanisms to enable data portability between service providers [123].

Concluding Remarks

Research in this paper has shown leading-edge quality of draft revised Convention 108 and its Additional Protocol to ensure an international common core system for safeguarding rights and freedoms of individuals and especially their right to privacy, in specific postmodern data processing conditions and a globalized environment. As such, efforts towards a review and modernization seem a natural progression of notable activities of the Council of Europe so far in the area of data and privacy protection. While taking into account that modernization is inspired by various different frameworks, in my research I focused on the European legal context, notably the European Union data protection framework. It has had a traditionally close connection with the relevant Council of Europe framework, and an influence on development of legislative frameworks also beyond Europe. I therefore also examined key developments in regulation of personal data and privacy protection at EU law level, whose groundbreaking standard-setting activities resulted in the accordingly advanced data protection enforcement systems. Analysis of the draft revised Council of Europe convention points to good similarity of proposed solutions that are already in force under EU law, and especially with respect to certain key proposals in the future EU general data protection framework. In other words, a good degree of inspiration for standard-setting solutions in the draft revised convention comes also from this angle and furthermore, mechanisms in proposed convention suggest ensured coherence between these two frameworks. This includes solutions proposed for data transfers across borders, which will require a consistent approach on contractual safeguards that are to facilitate international data transfers under both these frameworks.

The general nature of draft revised convention together with its new mechanisms to facilitate international data flows may well be key to its future success, in terms of accession by as many countries internationally and towards its eventually becoming a globally binding standard, which is the aspired goal at the Council of Europe. However, differences in implementation of safeguards to rights and freedoms of individuals, which need to be truly effective in practice, can also make all the change to the goals carried by this modernization. Harmonization through dissemination of best practice is in any case supported by important requirements and mechanisms, such as a reinforced international cooperation between the data protection supervisory authorities having necessarily stronger role and powers, as well as the specific role and functions of the future Convention Committee. At any rate, exciting and dynamic times in privacy and data protection worldwide are here to stay.

References

1. 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), Strasbourg, 8.11.2001; Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data approved by the Committee of Ministers, in Strasbourg, on 15 June 1999. Available online at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
2. Council of Europe Press Release, Uruguay becomes the first non-European state to accede to personal data protection Convention 108, 12.04.2013, Strasbourg, http://www.coe.int/t/dghl/standardsetting/DataProtection/News/Press-release-FINAL-Uruguay-revised_EN.pdf.
3. Council of Europe Committee of Ministers, Ministers' Deputies Decisions, CM/Del/Dec(2013)116, 1.2.2013, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) – Request by the Kingdom of Morocco to be invited to accede, 1160th meeting, 30.1.2013, Decisions adopted. Available online at: https://wcd.coe.int.
4. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] (T-PD), Modernisation of Convention 108, T-PD(2012) 4Rev3_en, Strasbourg, 29.11.2012, available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/ (further: Proposal), text of Preamble.
5. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23.9.1980, http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html.
6. Convention for the protection of individuals with regard to automatic processing of personal data: Explanatory Report, http://conventions.coe.int/Treaty/en/Reports/Html/108.htm, point II.
7. Explanatory Report – in [6], points 14-15, 90; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Explanatory Memorandum, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum, points 13-14, 18, 20.
8. Article 23 of the Convention 108, see Explanatory Report – in [6], point 90.
9. More details including the exceptions to this basic principle are stipulated in Article (12) of Convention 108.
10. Article 4 and Explanatory Report – in [6], point 38.
11. Article 11 of Convention 108.
12. Personal data concerning health or sexual life, personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data relating to criminal convictions may not according to Article 6 of Convention 108 be processed automatically unless the Party provides appropriate safeguards in domestic law.
13. Article 5 of Convention 108.
14. Article 7 of Convention 108.
15. Article 8 of Convention 108.
16. Such restrictions must be provided by law and they must constitute a necessary measure in the democratic society, in the interest of protecting State security, public safety, monetary interests of the State or suppression of criminal offences, or in the interest of protecting data subjects or rights and freedoms of others. For more details see Article 9 of Convention 108.
17. Article 10 of Convention 108.
18. Article 15(b) of the Statute of the Council of Europe, London, 5.5.1949. Available online at: http://conventions.coe.int/Treaty/en/Treaties/Html/001.htm.
19. Lee Bygrave, International Agreements to Protect Personal Data, in James B. Rule and Graham Greenleaf (Eds.), Global Privacy Protection. The First Generation, Edward Elgar Publishing Ltd., 2008, pp. 15–49 at p. 25.
20. Source: Council of Europe, http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal_instruments_en.asp.

21. Ministers' Deputies Decisions, CM/Del/Dec(2006)962, 2.5.2006, 962nd meeting, 26.4. 2006 (Decisions adopted). Available online at: https://wcd.coe.int/.
22. Council of Europe, Data Protection Day, http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day_en.asp; StaySafeOnline – National Cyber Security Alliance, Data Privacy Day, http://www.staysafeonline.org/data-privacy-day/about.
23. See, for example: Resolution calling for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data, 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel, 27-29.10.2010; The Madrid Privacy Declaration - Global Privacy Standards for a Global World, 3.11.2009, The 31st International Conference of Data Protection and Privacy Commissioners, Madrid, 4-6.11.2009; Montreaux Declaration - The protection of personal data and privacy in a globalised world: a universal right respecting diversities, The 27th International Conference of Data Protection and Privacy Commissioners, Montreaux, Montreaux, 14-16.9.2005. Resolutions adopted (up to 2013) are available online at: http://privacyconference2012.org/english/sobre-la-conferencia/antecedentes; http://privacyconference2012.org/.
24. See, for example: Council of Europe, Global Standards - Benefits for Benefits for CoE non-Member States, available at: http://www.coe.int/t/dghl/standardsetting/DataProtection.
25. See sources in [23].
26. The Madrid resolution adopted at the 31st International Conference of Data Protection and Privacy Commissioners (Madrid, 5.11.2009) welcomed these standards (Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data) and recognized their potential towards a binding international instrument. Available online at: http://privacyconference2012.org/english/sobre-la-conferencia/antecedentes.
27. Montreaux Declaration – in [23].
28. Martin, Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Advance Edited Version, A/HRC/13/37, 28.12.2009, http://www2.ohchr.org/ english/issues/terrorism/ rapporteur/docs/A_HRC_13_37_AEV.pdf.
29. This is according to interpretations of Article 17 of the International Covenant on Civil and Political Rights (16.12.1966), under which no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Furthermore, everyone has the right to the protection of the law against such interference or attacks. The Office of the UN High Commissioner for Human Rights interpreted protection of the right to privacy as guaranteed by this article to also cover personal data protection. This is because it entails a duty to regulate by law (automated) processing of information relating to individuals' private life, including effective measures to prevent unlawful processing thereof, that include the measures to ensure that this data are not used for a purpose that is not in line with the International Covenant. Protection of private life of individuals in this respect requires that individuals have the right to ascertain if their personal data are being processed as well as the right to ask for their correction, or deletion in cases of unlawful processing thereof. Office of the United Nations High Commissioner for Human Rights, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), 8.4. 1988, http://www.unhchr.ch/tbs/doc.nsf/0/23378a8724595410c12563ed004aeecd?Opendocument, especially point 10. In the context of relevant international (UN) legal sources it is here also necessary to point to Article 12. of the Universal Declaration of Human Rights (10.12.1948.), according to which no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation, and additionally, the right to the protection of the law against such interference or attacks is guaranteed to all. With respect to UN legal sources specifically relating to personal data protection, see the (non-binding) UN Guidelines for the Regulation of Computerized Personal Data Files, 14.12.1990, http://www.unhcr.org/refworld/docid/3ddcafaac.html.
30. Scheinin - in [28] at p. 34 (point 73).
31. For excellent research into this issue (including a more detailed look into Convention 108 and related developments) and plausibility to reach global standards in doctrine see, e.g. Christopher Kuner, An international legal framework for data protection: Issues and prospects, Computer Law & Security Review, Vol. 25, No. 4., 2009, pp. 307-317; Lee Bygrave, Privacy and Data Protection in an International Perspective, Scandinavian Studies in Law, 56, 2010, pp. 165–200; Graham Greenleaf, Global Data Privacy in a Networked World (October 14, 2011), in: Research Handbook on Governance of the

Internet, I. Brown, ed., Edward Elgar, 2012; UNSW Law Research Paper No. 2011-38. Available at SSRN: http://ssrn.com/abstract=1954296.

32. For excellent analyses see e.g.: Lee Bygrave, International Agreements to Protect Personal Data, in James B. Rule and Graham Greenleaf (Eds.), Global Privacy Protection. The First Generation, Edward Elgar Publishing Ltd., 2008, pp. 15–49, especially at p. 48; Christopher Kuner, An international legal framework for data protection: Issues and prospects, Computer Law & Security Review, Vol. 25, No. 4., 2009, pp. 307-317, especially at pp. 309-311; Bygrave – in [31], especially at pp. 181-182; Greenleaf – in [31], at p. 10.
33. See e.g. Bygrave – in [31], at pp. 181-182; Greenleaf – in [31], at p. 10.
34. Greenleaf – in [31], at p. 10. Additionally see Graham Greenleaf, The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108 (October 19, 2011), International Data Privacy Law, Vol. 2, Issue 2, 2012; UNSW Law Research Paper No. 2011-39; Edinburgh School of Law Research Paper No. 2012/12. Available at SSRN: http://ssrn.com/abstract= 1960299, at p. 31.
35. Greenleaf – in [34], at p. 32.
36. For a good analysis of certain problems identified with respect to current procedures and standards for accession, see Greenleaf – in [34], at pp. 25 et seq.
37. See also Resolution No. 3 on data protection and privacy in the third millennium, 30th Council of Europe Conference of Ministers of Justice, Istanbul, 24–26.11.2010, MJU-30 (2010) RESOL. 3 E, 26.11.2010. http://www.coe.int/t/dghl/standardsetting/minjust/mju30/MJU-30%20_2010_%20RESOL%203%20E %20final.pdf.
38. Jean-Marc Dinant, Cécile de Terwangne, Jean-Philippe Moiny,Yves Poullet and Jean-Marc Van Gyzeghem, Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques, T-PD-BUR(2010)09, http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD-BUR_2010_ 09%20FINAL.pdf.
39. Council of Europe, Modernisation of Convention 108: give us your opinion!, http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_E N.pdf; Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] (T-PD-BUR), Cécile de Terwangne and Jean-Philippe Moiny, Report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data, T-PD-BUR(2011)10 en, 21.6.2011, Strasbourg, http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_en.pdf; Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] (T-PD-BUR), Consultation concerning the modernisation of Convention 108: results, T-PD-BUR(2011) 01MOSrev6, Strasbourg, June 2011, http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_01_%20MOS6%20Results.pdf.
40. Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD-BUR), Draft Explanatory report of the modernised version of Convention 108 (based on the proposals adopted by the 29th Plenary meeting of the T-PD), T-PD-BUR (2013)3EN, Strasbourg, 31.1.2013, http://www.coe.int/t/dghl/standardsetting/dataprotection/, point 3.
41. OECD, The 30th Anniversary of the OECD Privacy Guidelines, www.oecd.org/sti/privacyanniversary.
42. Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data approved by the Committee of Ministers, Strasbourg, 15.6.1999.
43. According to the Commission the "negotiation is an opportunity to export the EU's gold standard of data protection beyond the borders of the Member States". Europa Press Releases RAPID, Commission to renegotiate Council of Europe Data Protection Convention on behalf of EU, MEMO/12/877, Brussels, 19.11.2012, http://europa.eu/rapid/press-release_MEMO-12-877_en.htm#PR_metaPressRelease_bottom.
44. 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.
45. Bygrave – in [31] at p. 187. Also see Bygrave – in [32] at p. 47

46. Greenleaf – in [34] at p. 14. For comprehensive studies on data protection/privacy laws and other relevant frameworks outside the EU and the degree of influence of "European standards", see: Greenleaf – in [34], Greenleaf – in [31]. Additionally see Bygrave – in [31].
47. Greenleaf - in [31] and [34], Bygrave – in [31], especially at p. 183.
48. For more details see Chapter IV of the General Data Protection Directive.
49. Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement, Official Journal L 296, 23.11.2000, pp. 41-43.
50. Article 3 and recital 27 of the General Data Protection Directive.
51. Recital 11 of the General Data Protection Directive.
52. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal L 24, 30.1.1998, pp. 1-8; see Article 1 (2) and recital 11.
53. Article 1 (2) of Directive 97/66/EC and recitals 3, 11.
54. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L 201, 31.7.2002, pp. 37-47; 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 L 337, 18.12.2009, pp. 11-36.
55. Recitals 5-6 of Directive on Privacy and Electronic Communications.
56. Charter of Fundamental Rights of the European Union, Official Journal C 326, 26.10.2012, pp. 391-407; Article 6(1) of the Treaty on the European Union - Consolidated version of the Treaty on European Union, Official Journal C 326, 26.10.2012, p. 13. The Charter binds EU institutions, bodies and agencies, as well as Member States when implementing EU law (for more details see Article 51).
57. The right to respect of private life and communications in Article 7 of the Charter has same meaning and scope as Article 8 of the ECHR: „Explanations relating to the Charter of Fundamental Rights of the European Union", Official Journal C 303, 14.12.2007, pp. 17-35 at p. 20. For relevant CJEU case-law reflecting this see: C-400/10, PPU J. McB. v L. E. (2010), European Court Reports, I-08965, paragraph 53.
58. Consolidated version of the Treaty on the Functioning of the European Union", Official Journal C 326, 26.10.2012, p. 47.
59. 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; 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.
60. 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.
61. Article 91 of the proposed General Data Protection Regulation.
62. Art. 288 (2)-83) of the Treaty on the Functioning of the European Union.
63. For more details see Article 3 and recitals 20-21 of proposed General Data Protection Regulation.
64. See, e.g. analysis in: Nina Gumzej, Data Protection for the Digital Age: Comprehensive Effects of the Evolving Law of Accountability, Juridical Tribune, Vol. 2, Issue 2, December 2012, pp. 82-108, available at: http://www.tribunajuridica.eu/arhiva/An2v2/art7.pdf.
65. Council of Europe, Data Protection Day 2013, Strasbourg, 28.1.2013, http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD_documents/Data%20Protection%20Day%202013_28_01_2013_En.pdf.

66. Proposal – in [4].
67. Proposal - in [4].
68. Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD-BUR), Draft Explanatory report of the modernised version of Convention 108 (based on the proposals adopted by the 29th Plenary meeting of the T-PD), T-PD-BUR(2013)3EN, Strasbourg, 31.1.2013. Draft Explanatory Report is available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/ (further: Draft Explanatory Report).
69. Draft Explanatory Report - in [68], point 5.
70. Article 1 of the Proposal, point 14 of the Draft Explanatory Report.
71. This is guaranteed under Article 8 of the ECHR. For relevant case-law, see especially S. and Marper v The United Kingdom, (application nos. 30562/04 and 30566/04), judgment, Strasbourg, 4.12.2008, paragraph 103.
72. Draft Preamble (Proposal). In that respect see relevant case law of the Court of Justice of the EU: C-92/09 and C-93/09, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, (2010) European Court Reports, paragraphs 47-52.
73. Article 2(c) of the Proposal, additionally see Draft Explanatory Report, point 22.
74. Article 2(b) of General Data Protection Directive; Article 4(3) of proposed General Data Protection Regulation ("processing").
75. Data Protection Unit of the Secretariat General of the Council of Europe, Update on the Council of Europe Convention 108, Strasbourg, 10.1.2012, available at: http://fra.europa.eu/fraWebsite/symposium2012/docs/council-of-europe-convention-108-Polakiewicz.pdf.
76. Article 3 of the Proposal, compare with current Article 3, especially Article 3(2) of Convention 108 on declarations.
77. Draft Explanatory Report, point 28 (explanations on the exception of purely household/commercial activities); Article 2(2)(d) of the proposed General Data Protection Regulation.
78. See Article 2 (1) and (2) of proposed General Data Protection Regulation.
79. For more details see Article 9 of the Proposal (compare with current Article 9 of Convention 108).
80. Article 11 of the Proposal.
81. Article 4 of the Proposal, points 32-40 of the Draft Explanatory Report (compare with Article 4 of Convention 108).
82. For more details see Article 4(3) and Chapter V of the Proposal (compare with Chapter V of Convention 108).
83. For more details see especially Chapters III bis (Article 12bis) and IV of the Proposal (compare with Article 1 of Additional Protocol and Chapter IV of Convention 108).
84. See especially Chapters 6 and 7 of the proposed General Data Protection Regulation.
85. For case law of the Court of Justice of the European Union (CJEU) interpreting the requirements for independence of data protection supervisory authorities (according to the General Data Protection Directive), see: C-518/07, European Commission v Federal Republic of Germany, 9.3.2010, (2010) European Court Reports, I-01885; for a more recent judgment see: C-614/10, European Commission v Republic of Austria, 16.10.2012 (not yet published in European Court Reports, text available at: http://curia.europa.eu).
86. For more details see Article 12 of the Proposal. Also see Draft Explanatory Report , points 92-106.
87. See especially Articles 42-43 of Proposed General Data Protection Regulation.
88. In that respect see especially points 10 et seq in the Draft Explanatory Report.
89. Draft Explanatory Report, point 15.
90. Compare Article 2(d)-(f) of the Proposal with Article 2 (d),(e) and (g) of the General Data Protection Directive.
91. Article 2 (a) of the Proposal, Draft Explanatory Report, points 16 and 18, for more details see points 17, 19-21.

92. Article 2 (a), additionally see also recital 26 of the General Data Protection Directive. For related case law of the Court of Justice of the European Union, see: C-101/01, Criminal proceedings against Bodil Lindqvist, (2003) European Court Reports, I-12971, paragraph 27; C-70/10, Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs (SABAM), paragraph 51; C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers (Sabam) v Netlog NV, paragraph 49 (the latter two cases are not yet published in European Court Reports, text is available at: http://curia.europa.eu). Additionally, for extensive interpretation of the personal data concept according to the General Data Protection Directive (legally non-binding, but influential) see: Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, 20.6.2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
93. Compare with Article 4(1)-(2) as well as recitals 23-24 of the General Data Protection Regulation.
94. Unlike the articles (of directives, regulations), recitals have no independent binding force in EU law, but they can be highly helpful for explaining and interpreting them. Recitals will not apply if they are in conflict with the articles, however, if the article is unclear (and recital is clear), then the article will be interpreted according to the recital. Tadas Klimas and Jurate Vaiciukaite, The Law of Recitals in European Community Legislation, ILSA Journal of International & Comparative Law, 15, 2008. Available at SSRN: http://ssrn.com/abstract=1159604, at pp. 23-28; for relevant case law see e.g. C-308/97, Giuseppe Manfredi v Regione Puglia, (1998) European Court Reports, I-07685, paragraphs 29-30; C-162/97, Criminal proceedings against Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn, (1998), European Court Reports, I-07477, paragraph 54.
95. Article 5(2) of the Proposal.
96. Compare definition of consent in Article 4(8) of proposed General Data Protection Regulation (additionally see also Article 7 on conditions for consent) with explanations of consent according to Article 5(2) of the Proposal, in point 43 of the Draft Explanatory Report.
97. Article 5(1), Draft Explanatory Report, point 39 (additionally see also text in points 40-41). Additionally see also Article 5(3)(b) of the Proposal.
98. Article 5 (3)(c), additionally see Draft Explanatory Report, point 50.
99. Article 7bis of the Proposal (compare with Article 8 of Convention 108).
100. Article 9(1) of the Proposal.
101. See Article 14 of proposed General Data Protection Regulation and especially points 64-65 of the Draft Explanatory Report (in relation to Article 7bis of the Proposal).
102. Article 9(1) of the Proposal.
103. Draft Explanatory Report, point 69.
104. Recommendation CM/Rec(2010)13 of the Committee of Ministers to Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23.11.2010.
105. For example, Article 12(a), 3rd subparagraph and Article 15 of the General Data Protection Directive (automated individual decisions); extended information requirements (right of access of data subject) according to Article 15 of proposed General Data Protection Regulation, Article 19(1) on the right to object, Article 20(4) on information requirements and measures based on profiling (proposed General Data Protection Regulation).
106. Article 6 of the Proposal. For more details, see explanations in points 52-57 of the Draft Explanatory Report.
107. Article 7(2) of the Proposal.
108. Article 9(1) of the Proposal.
109. For more details see Article 4(9) and Articles 31-32 of proposed General Data Protection Regulation.
110. This was introduced with the amendment of the Directive on Privacy and Electronic Communications in 2009, for more details see Article 2 i and Article 4 (3)-(5).
111. Draft Explanatory Report, points 60-62.
112. Article 8bis of the Proposal.
113. Article 7(1) of the Proposal.
114. Article 17 of the General Data Protection Directive.

115. See e.g. Articles 26-30, 33-37 of proposed General Data Protection Regulation.
116. Analysis of author is available in: Gumzej – in [64].
117. As to the proposed General Data Protection Regulation see especially its Article 22.
118. Article 33 of proposed General Data Protection Regulation.
119. Article 23 of proposed General Data Protection Regulation.
120. Draft Explanatory Report, point 81.
121. Points 77-79 of the Draft Explanatory Report.
122. Draft Explanatory Report, point 77 – with respect to Article 8bis (1) of the Proposal. For more details on data protection officers under the proposed General Data Protection Regulation, see its section IV.
123. Draft Explanatory Report, point 79 - with respect to Article 8bis (3) of the Proposal. For more details on data portability according to proposed General Data Protection Regulation, see its Article 18.