COMPUTER LAW & SECURITY REVIEW 30 (2014) 633–642

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition

Paul de Hert [a,*], *Vagelis Papakonstantinou* [a,b]

[a] *Free University of Brussels (VUB-LSTS), Belgium*
[b] *MPlegal, Athens, Greece*

Keywords:
Data Protection Convention 108
Council of Europe Data Protection
Global data protection standard

ABSTRACT

The year 2010 set an important milestone in the development of data protection law in Europe: both Europe's basic regulatory texts, the EU Data Protection Directive and the Council's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), were placed at an amendment process, having served individual data protection for many years and witnessed in the meantime technological developments that threatened to make their provisions obsolete. After briefly presenting Convention 108, the analysis that follows will highlight the Council's data protection system currently in effect as well as developments relating to the Convention's amendment so far with the aim of identifying improvements and shortcomings. While doing this two separate points of view shall be adopted: at first a micro point of view will attempt to identify improvements and shortcomings through an 'insider' perspective, that is, judging only the merits and difficulties of the draft text at hand. Afterwards a macroscopic view will be adopted, whereby strategic issues will be discussed pertaining to the important issue of the relationship of the suggested draft with the EU data protection system, as well as, the same draft's potential to constitute the next global information privacy standard.

1. Introduction

The year 2010 set an important milestone in the development of data protection law in Europe: both Europe's basic regulatory texts, the EU Data Protection Directive[1] and the Council's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Council of Europe Data Protection Convention or Convention 108),[2] were placed at an amendment process, having served

* *Corresponding author*. Law Science Technology & Society (LSTS), Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussels, Belgium.
E-mail addresses: paul.de.hert@vub.ac.be, paul.de.hert@uvt.nl (P. de Hert), vpapakonstantinou@mplegal.gr (V. Papakonstantinou).

[1] 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* L 281, 23/11/1995.

[2] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28. I.1981.

http://dx.doi.org/10.1016/j.clsr.2014.09.002

individual data protection for many years and witnessed technological developments that threatened to make their provisions obsolete. The year before (2009), the other basic international (non-binding) data protection text, the OECD Guidelines,[3] also entered a review process,[4] making therefore this period a turning point for data protection globally.[5]

Admittedly, each one of the above three texts fared differently in the data protection scene over the past few decades, despite their common origins – if not principles. The EU Data Protection Directive went on to constitute the *ad hoc* global data protection standard that, by means of its *adequacy* criterion, has been actively exported across the globe. The OECD Guidelines remained a voluntary text that gained international recognition but however offered limited substance to the global data protection discussion. From its part, the Council of Europe Data Protection Convention took up an ambivalent role: it constituted a binding text that however came to be addressed predominantly to states that are also EU Members – and thus committed to the EU Data Protection Directive's provisions. Its amendment process now under way, as well as the option for ratification by non-European states, could signal an attempt for it to constitute the next global standard (and thus replace in this regard the EU instrument). However, as it will be demonstrated in the analysis that follows, in order to accomplish this bold(-er) steps and a (more) radical approach shall be eventually needed.

After briefly presenting the Council of Europe Data Protection Convention, the Council's data protection system currently in effect and developments relating to the Convention's amendment so far (under parts 2, 3 and 4), improvements and shortcomings of the draft amended Convention shall be highlighted in the analysis that follows. Inevitably, while doing this two separate points of view shall be adopted: as regards parts 5–8, improvements and shortcomings shall be identified adopting an 'insider', micro point of view that is, judging only the merits and difficulties of the draft text at hand. On the other hand, in parts 9 and 10 a macroscopic view will be adopted, whereby strategic issues will be discussed pertaining to the important issue of the relationship of the suggested draft with the EU data protection system, as well as, the same draft's potential to constitute the next global information privacy standard.

2. The Council of Europe Data Protection system

Work in the Council of Europe in the field of data protection began as early as in 1968[6]; the motivation lay expressly within advances in information technology.[7] In early 1981, the Council of Europe Data Protection Convention was formally introduced and came into effect on 1 October 1985 for the states who had ratified it. The Convention constituted the first at that time (and only, for almost a decade) legally binding international instrument in the data protection field: it requires its signatory states to apply its principles in their domestic legislation.

An analysis of the actual provisions of the Council of Europe Data Protection Convention exceeds the purposes of this paper; here it is enough to be noted that the Convention includes in its text the Fair Information Principles (among others, the purpose limitation principle, the fair and lawful processing principle, the adequacy principle, the data quality principle etc.) as well as the special set of data protection rights for individuals (to information, access and rectification).[8]

'Sensitive' personal data are acknowledged and specially protected. The Convention is addressed to the private and the public sectors alike, including law enforcement agencies. It also was the first to formally establish the *adequacy* criterion for the exchange of personal data between two countries. A point perhaps worth mentioning, particularly with regard to the potential international role of the amended Convention (see below under 10), refers to the fact that during its drafting observer status was granted to the OECD, Australia, Canada, Japan and the United States. In addition, co-operation with the, then, EEC, now EU, was also formally secured.[9]

In the years that followed the Council of Europe furthered its Convention through the release, in 2001, of an Additional Protocol regarding supervisory authorities and transborder data flows (that was however significantly influenced by the

[3] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.

[4] The other international instrument, the UN Guidelines, has been, lamentably, left behind – perhaps a missed opportunity towards true international information privacy regulation (see P. De Hert & V. Papakonstantinou, "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?," *I/S: A Journal of Law and Policy for the Information Society* 9, no. 2 (2013): 271–327.).

[5] See for an overview of recent proposals for modernizing information privacy law in the USA, the European Union, Australia and New Zealand: G. Gunasekara, "Paddling in unison or just paddling? International trends in reforming information privacy law", *International Journal of Law and Information Technology*, 2013, pp. 1–37.

[6] See also C. J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992); C. Bennett & C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, [2nd and updated ed.]. (Cambridge Mass.: MIT Press, 2006). In practice, the cross border development of data privacy was realised through work in the OECD and the Council of Europe, as well as, through "*a closely knit group of experts in different countries [that] coalesced, shared ideas, and generated a general consensus about the best way to solve the problem of protecting the privacy of personal information*" (C. Bennett & C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, [2nd and updated ed.]. (Cambridge Mass.: MIT Press, 2006), 8, 112); see also C. Raab & E-J. Koops, "Privacy Actors, Performances and the Future of Privacy Protection", in S. Gutwirth et al. (eds.), *Reinventing Data Protection?*, Springer Science, 2009, 209.

[7] See Explanatory Memorandum, 4.

[8] See also P de Hert & E Schreuders, "The Relevance of Convention 108" (presented at the European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future, Warsaw, 2001), 34ff.

[9] See Explanatory Memorandum, 14 and 16.

EU Data Protection Directive, see below under 10).[10] Before that, an amendment in 1999 opened up the way for the EU to accede to the Convention as well. In addition, in order to adapt the general principles set out in the 1981 Convention to the specific requirements of various personal data processing sectors, a number of recommendations dealing with case-specific subjects have been adopted by the Council of Europe on issues ranging from medical databanks (adopted in 1981) and police records (adopted in 1987) to the protection of privacy on the internet (adopted in 1999), profiling (adopted in 2010) and social networking services (adopted in 2012). These recommendations have the advantage of being easier to draw up, to adopt and to implement: instead of signature and ratification by each of the Member States, they only require unanimous adoption by the Committee of Ministers.

Administrative work with regard to the Council of Europe Data Protection Convention purposes is conducted within its, so-called, T-PD Committee. This committee formally holds a consultative role, whereby it may make "*proposals with a view to facilitating or improving the application of the Convention*" or "*proposals for amendment of this convention*".[11] Although over the years the T-PD Committee did not prove as active as its EU counterpart (the Article 29 Data Protection Working Party), its work is central for the purposes of this paper in the sense that it is the draft amended Convention as prepared by it, in late 2012, that constitutes the basis of this analysis.[12]

3. Enduring relevance of the Council of Europe Data Protection Convention

Before elaborating upon the amendment process of the Council of Europe Data Protection Convention and its most significant points with regard to individual data protection, brief mention ought to go to the, at least five, reasons why, despite of its age, it still remains relevant in today's personal data processing environment.

The first reason pertains to the fact that it is a binding international legal instrument. Until today there exists no other instrument of a similar status: the OECD, APEC (Asia Pacific Economic Cooperation) and UN Guidelines are voluntary in nature and the EU Data Protection Directive, while assessing the adequacy of data protection regimes in third countries, does not oblige them in any way. The Council of Europe itself has 47 Member States and the number of signatory states to the Convention may increase even further, because it is open also to non-member states.

The second reason refers to the fact that its text, in its current wording, is fairly flexible. Particularly if compared with the formal and strict EU Data Protection system, the Council of Europe Data Protection Convention affords its signatory states with a fair amount of flexibility, particularly taking into consideration its mandatory nature.

The third reason why the Council of Europe Data Protection Convention still remains relevant after some 35 years since its release refers to the fact that, even for EU Member States, it remains the only mandatory text regulating the processing of law enforcement agencies. All personal data processing is to be governed by its provisions, including therefore both public and private sector as well as that of law enforcement agencies.

Finally, the fourth (and perhaps even fifth) reason refers to the Convention's closeness to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and to the European Court of Human Rights (ECtHR). As far as the Convention's legal basis is concerned, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) introduces an individual right to privacy – in fact, it was the limitations acknowledged by the Council of protecting individual privacy through the broad wording of Article 8 ECHR that led to the introduction of a specialized instrument, Convention 108.[13] Data protection therefore, at least as far as the Council of Europe is concerned, emerged as a spin-off of an existing fundamental human right, the right to privacy.[14]

In addition to the ECHR, the Council of Europe has instituted a judicial procedure which allows individuals to bring actions against governments, if they consider that their rights and freedoms have been breached. Complainants have direct access to an international court, the European Court of Human Rights in Strasbourg (ECtHR). With regard to the data protection purposes, the ECtHR, applying a '*dynamic and broad*' interpretation of the Convention, has derived a right to data protection from Article 8 of the ECHR, releasing over the years significant case law that furthered individual data protection particularly in these cases where EU law was, by definition, excluded (namely, law enforcement agencies' personal data processing).[15]

4. The Convention amendment process – the hidden policy options

The process for the amendment of the Council of Europe Data Protection Convention was formally initiated in 2010, one year

[10] See P. de Hert & E. Schreuders, "The Relevance of Convention 108," 43.

[11] See Article 19 of Convention 108.

[12] Modernisation of Convention 108, The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD), T-PD(2012)Rev4, Strasbourg, 29.11.2012 (the '*draft amended Convention 108*').

[13] See P. De Hert & S. Gutwirth, Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence', Institute for Prospective Technological Studies-Joint Research Centre, Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN.

[14] P. De Hert & S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembrourg: Constitualisation in Action," in *Reinventing Data Protection?*, ed. S Gutwirth et al. (Dordrecht: Springer Science, 2009), 3–44.

[15] P. De Hert & S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembrourg: Constitualisation in Action," in *Reinventing Data Protection?*, ed. S Gutwirth et al. (Dordrecht: Springer Science, 2009), 3–44; see also European Court of Human Rights, National Security and European Case Law, 2013, par. 129–135.

before its 30th anniversary. Conveniently, Article 21 of the Convention prescribes in detail the process for its amendment: changes may be proposed by a Party, the Committee of Ministers or the T-PD. Subsequently a process of internal communications is described, that however needs to include the T-PD. The text of any amendment, after being approved by the Committee of Ministers, is then forwarded to the Parties for their own approval; any such amendment "*shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof*" (par. 6).

On 10 March 2010 the Council of Europe Committee of Ministers encouraged the modernisation of the Council of Europe Data Protection Convention; a relevant position paper was issued during the 32nd International Conference of Data Protection and Privacy Commissioners.[16] Work started in November 2010, within the T-PD, with most of 2011 being spent on public consultations. The T-PD organized several meetings in 2012, both at Bureau and Plenary level, over which the amendment proposals were formulated; the final draft amended Convention came out in late 2012. Subsequently a special committee was setup,[17] under the mandate to finalise the text in order to present before the Committee of Ministers.

A point to be noted refers to the fact that the Council does not provide an analysis of the draft amended Convention; in fact, the new text is provided on-line 'as it is', without, for instance, an explanatory memorandum of any kind (as, for instance, was the case with the EU data protection reform package[18]). Consequently, there is no way of knowing which policy options the Council faced while drafting it or the rationale behind its decisions. Similarly, there is no way of knowing which of the changes suggested in the new text are of central interest to the Council and which are not, or which issues have been contested within the T-PD working over the text and which have more or less met with general consensus. Only indirect inferences may be made by reference to the questions raised by the Council in its public consultation of 2011. Given the above, the policy options analysis *below* is necessarily subjective and may not coincide with the Council's priorities – whichever these may be.

At any event, a basic law-making choice of the Council refers to the fact that it apparently opted for an amendment of the Convention and not for its replacement. This decision might appear difficult to understand, given the grave technological and socio-economic changes that took place since 1981.[19] If one attempted to draw parallels, the EU thought that the EU Data Protection Directive, a text from 1995, needed to be replaced,[20] whereas the Council decided that the Convention, a text that came out a decade earlier, only needed to be partially amended. The drafters of the amended Convention wanted to preserve the structure and, if possible, the wording of the Convention as much as possible, despite of the fact that the new draft includes a whole new chapter and several new articles in comparison to the one in effect today.[21] However, this preference could ultimately affect the quality of the amendments to be adopted.

Other law-making options that the Council faced may be derived through the public consultation it released.[22] The Council evidently contemplated upon retaining the Convention's "*technologically neutral' approach, which keeps it general and simple'* or preparing a more detailed text; respondents opted for a simple and general approach, that will stand the test of time and also make it possible for third countries to accede to the Convention.[23] Bizarrely, however, with regard to the relationship between the amended Convention and the, far stricter and more formal, EU data protection system '*a great many contributors argue[d] that the work of modernising the Convention should be carried out from a concern to achieve the greatest possible consistency with the protection rules laid down by the European Union (mainly Directive 95/46). Thus in many cases replies were guided by this concern to align the text of the Convention with that of the European directive. The work of modernising that directive, currently in progress, should be monitored so as to ensure that discrepancies between the texts do not arise*'.[24] The issue of the relationship between Convention 108 and the EU data protection system, and the risks it might create to the former, shall be elaborated in detail later (see *below*, under 10).

Finally, another policy option refers to the amended Convention scope, in particular with regard to whether the personal data processing of law enforcement agencies should continue to be regulated by its provisions. We saw (see *above*, under 2) that the Convention remains the only text in Europe that regulates *all* processing, including security-related personal data processing in its signatory states. Respondents to the Council consultation

[16] *Council of Europe response to privacy challenges – Modernisation of Convention 108*, position paper distributed at the 32nd International Conference of Data Protection and Privacy Commissioners, 27–29 October 2010, Jerusalem, Israel.

[17] The Ad Hoc Committee on Data Protection (CAHDATA), CAHDATA(2013)TOR, Strasbourg, 10 July 2013.

[18] See European Commission, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final.

[19] Given also that it was well aware of the Convention's numerous shortcomings, see J-M Dinant, C de Terwangne & J-P Moiny, 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 (Strasbourg: Conseil de l'Europe – T-PD BUR, 2010).

[20] By a General Data Protection Regulation (GDPR), currently under negotiation (see European Commission, Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11final and also updates on the EU data protection reform at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm).

[21] Chapter IIIbis; altogether, the new draft includes 8 chapters and 30 articles, for the time being parenthetically numbered (using the 'bis' system).

[22] Council of Europe, Modernisation of Convention 108: Give us your opinion, February–March 2011.

[23] Council of Europe, T-PD Bureau, 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 June 2011, par.7.

[24] Council of Europe, T-PD Bureau, 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 June 2011, par. 6.

unanimously agreed that this had to be maintained,[25] a fact also depicted in the amended Convention text.

5. First major improvement: automated *and* manual processing is regulated

By regulating (only) automated personal data processing, the (original) Council of Europe Data Protection Convention made an important distinction that was perhaps justified back in 1981,[26] but, in the light of regulatory developments that followed, threatens to undermine the level of protection afforded to individuals by its provisions.

The self-restriction of scope to the electronic environment only is not unjustified, given that it is exactly the advent of information technology that led to the creation of the data protection field of law – before that personal life was protected in other ways.[27] However, when the basic regulatory texts for data protection were being elaborated, in particular the EU Data Protection Directive, it was considered advisable, in view of the fact that in the early nineties several EU Member States were in possession of files on individuals still in manual (paper) format, to extend the scope of data protection instruments (at least in the EU) not only to all automated processing but also to "*the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*" (Article 3.1).[28] Despite the straightforward origins of this distinction, when applied in practice it came to create substantial difficulties,[29] the elaboration of which largely exceeds the purposes of this paper. At this point it is enough to be noted that the inclusion of paper files is by now considered *acquis* in data protection law – and admittedly warrants a complete protection in those countries that have not yet computerized all their files.

The amended Convention, in view of wishing to become the new global standard offering comprehensive data protection on a standalone basis (see *below* under 10), could not possible continue being self-limited only to automated processing. To this end, not only its title has changed with this in mind, but also the relevant provisions on its scope make no mention whatsoever to whether personal data need to be stored electronically or not in order for it to apply.[30]

6. Second major improvement: consent as a legitimate basis

The (original) Council of Europe Data Protection Convention did not acknowledge individuals' consent as a lawful basis for the processing of their personal data. This may come as a surprise in the contemporary personal data processing environments where consent, both in and out of Europe, occupies a central spot in relevant discussions, evoking numerous and heated debates on the details of its admissibility.[31] Nevertheless, that did not seem to have been a priority back in the early 1980s and late 1970s, when the original Convention text was devised: in fact, nor the OECD Guidelines[32] or the UN Guidelines[33] (that came in 1990 but ought to be examined as same, first-generation, data protection texts) make any particular mention to individual consent or, for the same purposes, to the requirement for legitimate grounds for personal data processing. In fact, this approach was adopted much later, in the text of the EU Data Protection Directive (in Article 7).

It is difficult today to imagine why consent in particular and also the broader issue of legitimate grounds for personal data processing were left unaddressed back in 1980. Is consent not a logical tenet of the idea of informational self-determination, as was outlined by the Working Party 29 in 2011?[34] Fear for imposed take it or leave it-choices, data subjects' limited bargaining power and inability to assess the

[25] Council of Europe, T-PD Bureau, 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 June 2011, par.9.

[26] Essentially, even its official title, "*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*", confirms this choice. The restriction of its scope to the automated (electronic) environment only is stated expressly both in its scope, "*the Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors*" (Article 3.1), as well as in its explanatory memorandum, where the justification that led to its adoption is laid down. See, for instance, paragraphs 1 and 5. Admittedly, signatory states had the option to also apply the convention "to personal data files that are not processed automatically" (Article 3.2(c)).

[27] See G. González-Fuster, *The Emergence of Personal Data as a Fundamental Right in the EU*, Springer, Dordrecht, 2014.

[28] See also U. Dammann & S. Simitis, *EG-Datenschutzrichtlinie, Kommentar*, Nomos, 1997, pp. 120ff.

[29] See, for instance, the Lindqvist case, Court of Justice C-101/01, 6 November 2003. See for a Belgian example excluding many, not to say most non-automatic files: a judgment, of 16 May 1997, of the Belgian Supreme Court (Cour de Cassation) that held: "There can only be a filing system, if a systematical access to the set of personal data is enabled through the logically structured manner in which it is assembled and stored. A set of personal data that does not enable in any way to process, modify, erase or disseminate the data it contains, nor to store these personal data in a durable manner, in view of the systematic access thereto is not a filing system, even though it may be logically structured.". See the annotation to this judgment by J. Dumortier via http://www.anthologieprivacy.be/sites/anthology/files/Hof_van_Cassatie%2C_16_mei_1997.pdf.

[30] See its Article 3, where by now only processing executed for household purposes is excluded.

[31] See, for instance, Ian Kerr et al., "Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent," in *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, ed. Ian Kerr (Oxford University Press, 2009) pp. 5ff, G. Zanfir, "Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law" in S Gutwirth, R. Leenes & P. De Hert (eds.), *Reloading Data Protection – Multidisciplinary Insights and Contemporary Challenges* (Springer, 2014), pp. 237ff.

[32] In the OECD Guidelines of 1980 admittedly mention is made to consent, in Articles 7 and 10, but within the basic processing principles context and not as a legal basis for personal data processing.

[33] Here too, as is the case with the OECD Guidelines, consent is acknowledged but only within the processing principles context (in Article 3).

[34] Article 29 Data Protection Working Party Opinion 15/2011 on the definition of consent WP 187 (2011) 15.

privacy risks might explain the matter.[35] It might also be that the drafters of the original version of Convention treated data protection more as a human right and less as a technical set of rules for personal data processing. In other words, perhaps they did not believe that consent was an issue in the data protection context any more than it is an issue in any other human rights context[36]; therefore only the circumstances under which processing actually happened were regulated, by the general data processing principles. An additional level of control, in the form of whether legitimate reasons for such processing existed and whether the data subject has given consent, was not introduced. This older approach, – not talking about consent or legitimacy in general – is not without risks, since it opens the ground for ubiquitous and constant personal data processing: if no individual consent exists nor any law prescribes it and still personal data processing is allowed, then the contemporary data protection edifice is turned upside down: it does not grant rights to individuals but rather places obligations upon data controllers.

Such an important, additional restriction to personal data processing was indeed introduced by the EU Data Protection Directive. It is important at this stage to analyse briefly how consent operates in the EU data protection law context: personal data processing may take place only if one of the altogether six legal grounds conditions is met: individual consent is listed explicitly among them. If no consent or one of the other legal grounds exists then no personal data processing whatsoever may take place. The discussion on the basic data protection principles (e.g. whether data have been collected lawfully and fairly, are proportionate to the purpose of the processing etc.) comes later into play, only if existence of a lawful basis for the processing has been established.[37] If such basis is not there then the discussion over the basic data processing principles is irrelevant; lack of a legitimate ground for the processing cannot be amended in any way at a later stage. It is in this way that the mechanics of EU personal data processing are drafted (and shall probably continue to be so, in view of the wording of the draft Regulation in its Article 6).

Gunasekara observes that only today a global consensus is emerging as to its proper role,[38] although the EU reform package goes well beyond other reform proposals in addressing the place of consent by detailing amongst others the place of children's consent, withdrawal of consent and employee consent. The Council of Europe is apparently hooking in on this trend to address consent.[39] Consequently, the draft amended Convention expressly asks for a legitimate basis for individual personal data processing to take place; consent is one of the two alternatives to this end. As per its Article 5.2 "*each party shall provide that data processing can be carried out on the basis of the free, specific, informed and [explicit, unambiguous] consent of the data subject or of some legitimate basis laid down by law*". In this way, the Council of Europe Data Protection Convention moves away from its, admittedly more open, past approach, without, however also elaborating further on the details on consent, as for instance provided for in the EU data protection reform texts.

7. Third major improvement: the principle of accountability

The principle of accountability thus requires controllers to actively demonstrate compliance and not merely wait for data subjects or supervisory authorities to point out shortcomings[40]: data controllers are liable for their personal data processing, so they have to implement all measures at their own initiative in order to warrant, and be able to prove at all times, the lawfulness of their actions (for instance, by means of keeping internal documentation, appointing data protection officers or conducting impact assessments).[41]

In today's data protection reform discussions, the principle of accountability is one of the spearheads. One author rightly observes that European doctrine does not regard accountability as a stand-alone principle but, rather, as aimed at ensuring compliance with the other principles and containing two elements: adequate internal measures to ensure compliance and demonstrating externally how this has been accomplished.[42] In some writings and reform proposals on accountability outside Europe accountability is seen as an autonomous principle that has the particular charm of compensating for weaknesses in the application of other data protection principles: more accountability is then the answer to, for example, transfer of data to countries without adequate data protection, or, to business practices in collecting data

[35] G. Gunasekara, "Paddling in unison or just paddling? International trends in reforming information privacy law", *International Journal of Law and Information Technology*, 2013, 26–28 with ref. to D. J Solove, *Understanding Privacy*, Harvard: Harvard University Press, 2008, 73.

[36] See on the 'under theorized' status of consent and waiver of rights in human rights law, O. De Schutter, 'Waiver of Rights and State Paternalism under the European Convention on Human Rights', *N. Ir. Legal Q.*, 2000, vol. 51, 481–493.

[37] Of course, once a legitimate ground is found, then the principles are applicable – consent is not an overriding reason to process personal data outside the basic data protection principles of Article 6 of the EU Data Protection Directive (see S. Gutwirth, "Short Statement about the Role of Consent in the European Data Protection Directive," *The Selected Works of Serge Gutwirth*, 2012, http://works.bepress.com/serge_gutwirth/80).

[38] G. Gunasekara, "Paddling in unison or just paddling? International trends in reforming information privacy law", *International Journal of Law and Information Technology*, 2013, 26.

[39] This shortcoming of the Council of Europe Data Protection Convention was identified also in its lacunae report. See J-M Dinant, C de Terwangne & J-P Moiny, *Rapport sur les Lacunes de La Convention N° 108*, p. 29.

[40] European Union Agency for Fundamental Rights (FRA) & Council of Europe, *Handbook on European data protection law*, Luxembourg, Publications Office of the European Union, 2014 (second edition), 77.

[41] See also work undertaken on this matter by the Article 29 EU Data Protection Directive Working Party, *Opinion 3/2010 on the principle of accountability*, 13 July 2010.

[42] G. Gunasekara, "Paddling in unison or just paddling? International trends in reforming information privacy law", *International Journal of Law and Information Technology*, 2013, 22.

that do no allow effective individual control by the data subjects.[43]

The willingness to incorporate some idea of accountability seems to be a global phenomenon and in Europe partly follows from the case law on privacy developed by the European Court on Human Rights.[44]

The Council of Europe Data Protection Convention does not expressly acknowledge the principle of accountability in its text. Although little doubt is generally left to the fact that it is the data controller who is the prime recipient of the Convention's obligations, the fact that this is not stated expressly in its text has been considered a major shortcoming affecting the level of protection afforded to individuals.[45]

This has been amended in the text of the draft amended Convention: for the time being, Article 8bis sets that "*Each Party shall provide that the controller, or where applicable the processor, shall take at all stages of the processing all appropriate measures to implement the provisions giving effect to the principles and obligations of this Convention and to establish internal mechanisms to verify and be able to demonstrate at least to the supervisory authorities provided for in Article 12bis of this Convention the compliance with the applicable law*". In this way the principle of accountability is expected to become embedded in the Council of Europe environment. Although a number of issues need perhaps to be further elaborated (for instance, the partition of liability between the controller and the processor or the particular mechanisms that need to be implemented by data controllers), the fact remains that the Convention has joined other supranational data protection regulatory instruments in placing upon data controllers the expectation to comply, and be able to prove so, with data protection legislation.

8. Fourth major improvement: the incorporation of the requirement for a supervisory authority

Despite the fact that state data protection acts already enacted by the end 1970s had adopted the regulatory model whereby an independent state authority was to be setup to monitor compliance with the provisions of the new law (a Data Protection Authority), the Council did not take that, perhaps bold at the time, step: the Council of Europe Data Protection Convention did not formally require the establishment of such an authority. On the contrary, signatory states only had to "*designate one or more authorities*" for mutual assistance purposes.[46] Such authorities expressly need not be "data protection authorities".[47] The requirement for the establishment of a data protection authority came relatively late, in 2001 through Article 1 of its Additional Protocol. However, it must be kept in mind that signatory states may well choose to ratify the Convention itself and not the Additional Protocol.[48]

The Council's viewpoint that a Data Protection Authority is an essential data protection instrument is illustrated in the text of the draft amended Convention 108. Under its Chapter III the provisions of the Additional Protocol are suggested to be incorporated into the main Convention: "*Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles of this Convention*" (Art. 12bis.1). In addition, their powers and warranties for their operation are expanded, perhaps in a way that much resembles not only the EU Data Protection Directive but also (simultaneous) discussions for the EU GDPR.[49] In essence, what Chapter III describes is a new administrative agency that will not only monitor compliance within its jurisdiction but will also be a participant in all data protection decision-making within the state concerned: "*such authorities: a. have powers of investigation and intervention; b. perform the competences relating to transborder data flows [...]; c. may pronounce decisions necessary with respect to domestic law measures giving effect to the provisions of this Convention and in particular to sanction administrative offences; d. have power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the provisions of this Convention; e. are responsible for raising awareness of and providing information on data protection*" (Article 12bis.2). In this context, independence is crucial: "*The supervisory authorities shall perform their duties and exercise their powers in complete independence, they shall neither seek nor accept instructions from anyone*" (Article 12bis.4).

All of the above are important, substantial powers for a newly established organization. Outside the EU, whose Member States are accustomed to such a model for many years, this might prove an insurmountable difficulty for ratification of the new Convention 108 altogether: by incorporating the relevant provisions in its main text and formalizing

[43] "If it is impractical to provide Individual Control, these companies should ensure that they implement other elements of the Consumer Privacy Bill of Rights in ways that adequately protect consumers' privacy. For example, … such companies may need to go to extra lengths to implement other principles such as Transparency—by providing clear, public explanations of the roles they play in commercial uses of personal data—as well as providing appropriate use controls once information is collected under the Access and Accuracy and Accountability principles to compensate for the lack of a direct consumer relationship" (The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Washington, February 2012) quoted by G. Gunasekara, "Paddling in unison or just paddling? International trends in reforming information privacy law", *International Journal of Law and Information Technology*, 2013, 12).

[44] See more in detail: P. De Hert, 'From the Principle of Accountability to System Responsibility – Key Concepts in Data Protection Law and Human Rights Law discussions', in F. Zombor (ed.), *International Data Protection Conference 2011*, Hungary, Hungarian Official Journal Publisher, 2011, 88–120 and 'Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law', in D. Guagnin (and others), '*Managing Privacy through Accountability*', Hampshire, Palgrave Macmillan, 2012, 193–232.

[45] See J-M Dinant, C de Terwangne & J-P Moiny, *Rapport Sur Les Lacunes de La Convention N° 108*, p. 48ff.

[46] See Article 13 of Convention 108.

[47] See Explanatory Memorandum par.73.

[48] As indeed happens in many cases, see the ratification table available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=2&DF=&CL=ENG.

[49] See Chapter VI of the GDPR.

as much as possible the data protection authority role the Council elevates the bar even higher, asking third countries interested to accede to the Convention that they not only apply a new set of rules within their jurisdictions but that they also introduce a powerful new agency within their state mechanisms. Maybe, if the Council opted for an "effective" rather than an "independent" supervisory authority, and left it to signatory states to decide on the actual means and measures, it would have served its international ambitions in a better way.[50] To paraphrase the European Court on Human Rights one could argue that human rights protection needs to be effective, not necessarily independent.[51] The latter contributes to the former, but is not an autonomous human rights requirement.

9. The relationship with the right to privacy and the EU data protection model

While it is perhaps early to identify shortcomings of the draft amended Convention 108, given that its final wording is yet to be established, two areas may already be highlighted as potentially problematic: the first pertains to its relationship with the right to privacy[52] and the second to its relationship with the EU data protection model.

The relationship between the right to privacy and the right to data protection in the text of Convention is not easy to determine: while in its preamble it is set that "*it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing*" and it is also recognised that "*it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples*", its Article 1 sets that "*the purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*", leaving therefore the exact relationship between the two to anybody's guess. However, this is probably understandable within the context of a text developed in the late 1970s, when data protection was perceived as a spin-off of the general right to privacy (even, as per the Convention, in the automated processing of personal data). In a perhaps more revealing way the ECtHR has, in what constitutes by now standard practice, derived its extensive case law on data protection based on the wording of Article 8 of the ECHR which only refers to the right to privacy.

However, the EU has by now moved ahead and emancipated the right to data protection from the right to privacy, awarding to the former an independent, standalone status in the text of its Treaty.[53] In this way the data protection purposes have become concrete, self-sufficient guiding principles for all EU legislation, rather than guidelines included in a Directive or derived indirectly from the general right to privacy. While it is understandable that Convention 108 could not possibly introduce a new right to data protection or add to the ECHR list, its text could benefit from a clearer wording distinguishing between the two.

The second area of potential difficulties for the draft amended Convention 108 refers to its relationship with the EU data protection model. While the 1981 draft essentially included an open model with significantly reduced restrictions in comparison to the EU data protection directive, its 2001 protocol brought the two models closely together. In 2001 the formal requirements for an EU-like DPA and EU-like data export restrictions were introduced in its framework. In this way, however, although data protection safeguards were perhaps strengthened, Convention 108 lost its flexibility that could allow it to be adopted by third countries that, while wishing for some data protection, did not necessarily agree with the formal and strict EU model.

The draft amended Convention is in itself a fairly detailed text that more or less follows the EU data protection model (and, indeed, at times certain GDPR ideas currently under processing in the EU).[54] While this policy option may be welcome from a data protection point of view, it deprives Convention 108 from the flexibility perhaps expected by non-EU countries in order to accede to it. Its added value is also

[50] In this context, see also the OECD Guidelines of 2013 approach, that specifically ask for establishment of "*privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis*" (Article 19c) – such authorities, however, need not necessarily be "independent".

[51] See Article 13 of the European Convention on Human Rights (right to an 'effective' remedy). Compare also with the new OECD Guidelines: On p. 59 you see that The OECD too introduced reference to (need to establish) privacy enforcement authorities and specifies that they should have the "governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis." See C. Levallois-Barth, "Legal Challenges Facing Global Privacy Governance", in C. Dartiguepeyrou (ed.), *The Futures of Privacy*, Fondation Télécom, Institut Mines-Télécom, 2014, (55–64), 59.

[52] See also C. de Terwangne, "The Work of Revision of the Council of Europe Convention 108 for the Protection of Individuals as Regards the Automatic Processing of Personal Data," *International Review of Law, Computers & Technology* 28, no. 2 (May 4, 2014): 118–30, http://dx.doi.org/10.1080/13600869.2013.801588.

[53] See P. De Hert & S. Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", in Gutwirth, S., Poullet, Y., De Hert, P., Nouwt, S., De Terwangne, C. (eds.), *Reinventing Data Protection?*, Berlin, Springer, 2009, 5–45; Orla Lynskey, "Deconstructing Data Protection: The'Added-Value' of A Right to Data Protection in the EU Legal Order", *International and Comparative Law Quarterly*, 2014, Volume 63, Issue 3, 569–597.

[54] If the two texts (the draft amended Convention 108 and the GDPR) are compared in their respective current wordings it may easily be established that the Convention has adopted fully the EU data protection system of legitimacy of the processing, data quality principles, establishment of data protection authorities, as well as, award of individual rights to be informed of, access and rectify data. Similarities may also be traced in less substantial parts, such as, adoption of the EU data protection actors (data controller/data processor/recipient – an act of semantic value), adoption of data breach notifications (Article 7.2 of Convention 108), the right not to be subject to automated decisions (Article 8a), or the introduction of impact assessments (Article 8bis).

questioned under this policy option, given that EU Member States have to live with a stricter data protection model anyway while third countries that would wish to ratify it could also opt for "adequacy" status in the Directive (or GDPR) context, if at least the two texts coincide to a considerable extent (see also the analysis that immediately follows, under 10).

10. The (explicit and underlying) ambition of the draft amended Convention 108 to become the global information privacy standard

The international scene lacks to-date a widely acceptable information privacy standard. While different approaches cannot even agree on terminology (data protection, information privacy, privacy etc.) suggestions for what should constitute the global relevant standard come from many places and many backgrounds. The EU has been actively promoting its own data protection system (that, disappointingly, acknowledges as *adequate* only the legal systems of altogether 12 countries until today). The Council has its own Convention, open to ratification by non-member states as well. APEC, from its part, promotes its own information privacy model. The OECD Guidelines could be used to the same end. In addition, a multitude of formal or semi-formal organisations have released their own set of rules, including anything from technical standards to attempts for an international treaty.

This fragmented environment indicates that the international community lacks a formal set of information privacy rules that would be open to anybody interested to subscribe while, at the same time, not connecting the enforcement of too rigid rules to such participation. Becoming such a next global information privacy standard was already an aim under the original Convention and is an explicit aim of the draft amended Convention. This statement is listed within its priorities[55] and is openly discussed within the Council of Europe. The already existing mechanism for ratification by non-member states remains intact. In addition, observer status during all stages of its release has been granted to a multitude of parties and countries, achieving thus a possibly participatory drafting process in the international context.[56] Interesting is that not only non-European states that may have an interest in accession but also certain international organisations (United Nations, Organization of American States, African Union, Economic Community of West African States, Association of Southeast Asian Nations, and APEC) were involved. . Apparently part of the CoE's global strategy was to engage significant regional organisations in the reform process Greenleaf labels this process as *globalization through regionalization*.[57]

It remains to be seen whether the Council of Europe will fulfil its global norm setting ambition. Perhaps the most important obstacle to this end is its close relationship to the EU data protection model discussed above. The draft amended Convention perhaps moves too closely to the EU Data Protection Directive (and also the GDPR) in order for it to become the next global information privacy standard. Third countries have known the EU model for two decades by now and the fact that only a handful among them has chosen to abide by its rules demonstrates a mistrust, if not to its subject-matter at least to its requirements. Formal and rigid requirements, for instance the establishment of a new powerful agency or the adoption of the "legitimate grounds plus basic principles" model for each personal data processing operation, perhaps discourage aspiring subscribers that may be unwilling or unable to adopt them at national level. Members of the international community are not at the same level of personal data processing among them neither do they adopt the same governance models within their respective national borders: a data protection model that is perhaps standalone but needs alien mechanisms and principles in order to operate may perhaps prove impossible to implement.

In addition it must be noted that for EU Member States that are also members of the Council the added value of the current draft amended Convention 108 is apparently limited. The norms are high, but not high enough: the EU Data Protection Directive and the GDPR will probably do a better (in the sense of being more detailed) work protecting individual data protection while the Directive on police processing covers by now the gap of law enforcement processing, taking away from Convention 108 its most important contribution today. Consequently, under current circumstances these Member States apparently take interest in the drafting process only in order to ensure that the Convention provisions do not contradict these of the GDPR also under negotiation (a connection that also helps to explain progress of works within the Council).

In view of the above difficulties, and threatened failure of the draft amended Convention 108 to address them, the authors feel that their older recommendation for establishment of a new international organisation to protect data privacy, that would at first apply the UN Guidelines that are broad enough to warrant international acceptance, retains its value.[58]

11. Conclusion: a global acceptable standard?

The act of drafting the amended Convention includes careful and clear goal-setting. There is not much in the newly

[55] See, for instance, the Council statement that "the Convention is the only existing international legally binding instrument which has the potential to be applied worldwide" (Council of Europe response to privacy challenges, Article 8bis), and also G Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108" (presented at the International Data Protection Conference 2011, Budapest: Hungarian Official Journal Publisher, 2011).

[56] Third parties (USA, Canada and others) participated in the public consultation (see Council of Europe, T-PD Bureau, 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 June 2011) and also were present in T-PD Plenary meetings.

[57] See in detail G Greenleaf, "'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?," [2013] 29 *Computer Law & Security Review* 433.

[58] See P. De Hert & V. Papakonstantinou, "Three Scenarios for International Governance of Data Privacy."

proposed Convention that does not point in this direction. In most cases careful balancing and regulating has been accomplished by its drafters, who have achieved to incorporate or implement such international trends as accountability, participation, consent and transparency and have laid the foundation for an updated document that addresses new developments. These points are discussed *above* and also got more extensive attention in Greenleaf's excellent 2013 analysis of the reform within the Council of Europe.

The one critical point highlighted in our contribution is about strategy. A new Convention on data protection for whom? EU countries? European states that are not in the EU but are in the Council? Non-European states that want to sign up to the Convention because of its balanced nature? Because members of the Council include EU states bound by the rules of the more strict and detailed data protection EU model, the amended Convention needs to tread carefully in order not to contradict that model in any way. Its added value lies elsewhere: to non-EU member states, regardless whether Council members or not (whether European or not), that have some or no data protection rules within their respective jurisdictions. EU member states will be provided soon with a detailed data protection solution to replace, and hopefully improve, their already comprehensive relevant schemes. Little help can be provided to them by the Council of Europe Data Protection Convention itself (other instruments of the Council data protection system, such as the ECHR or the Court, may fare differently). On the contrary, a lot can be done through Convention 108 for third, non EU, countries. Greenleaf summarizes this by referring to the Goldilocks test that the Council of Europe needs to pass: its proposed norms cannot be too high or low, neither cold or too hot.[59]

The current draft amended Convention instead of remaining abstract and technology-neutral, comes close to personal data processing details. The draft at hand is a detailed text – perhaps not as comprehensive as the GDPR but still detailed enough if compared to the OECD or the UN Guidelines. It is placed too close to the EU model, implementing its most basic elements, and can therefore be perceived from a non-EU point of view only as an introduction to warranting an 'adequacy' finding by the EU at a later stage. In this way, however, a great opportunity will be missed. There is no reason for the Council of Europe to be detailed at all – the EU instruments will do that for their direct recipients and also for those non-EU countries that care to join them. The added value of an amended Council of Europe Convention, and what is truly missing from the global data protection scene, would be to produce a text that is broad enough for all countries in the world to accept and still has binding power for everybody to actually implement. This would inevitably mean a level of abstraction and *laissez-faire*. Aspiring signatory states to the new Convention need to be provided with many options and choices as to the data protection model they wish to implement within their national borders. However, rather than moving towards this direction, the draft Convention at hand may be viewed as a shortened GDPR version. The Council will need bolder decisions (extensive text deletions and transfer of 'hot' issues to protocols[60]), if indeed its intention is to serve the international information privacy, and not the EU data protection, community.[61] Survival in a changing world implies adaptation, also for institutions. In today's landscape, with the EU arrogantly claiming more and more policy areas,[62] it remains to be seen whether the current strategy of respectful autonomy is successful.

[59] See G. Greenleaf, "'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?", 436.

[60] Of course we refer to the Council of Europe Cybercrime convention, where the controversial provisions on combatting child pornography were inserted in an additional, optional protocol.

[61] See our discussion *above* of the requirements for data protection to be independent or effective and of the 2013 OECD Guidelines that advance the requirement of effectiveness (and not independence). We observe in passing that these new guidelines equally do not include language on a "right to forget" or on "Privacy-by-design," concepts that are in the draft EU data protection regulation, and that may not be ready for globalization.

[62] Compare P. De Hert, G. González Fuster & E.-J. Koops, "Fighting Cybercrime in the Two Europes: The Added Value of the EU Framework Decision and the Council of Europe Convention", *International Review of Penal Law*, vol. 77, 2006, no. 3–4, 503–524.