Innovation: The European Journal of Social Science Research

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ciej20

The proposed Regulation and the construction of a principles-driven system for individual data protection

Paul de Hert [a], Vagelis Papakonstantinou [a], David Wright [b] & Serge Gutwirth [a]

[a] Vrije Universiteit Brussels - Tilburg University (TILT), Brussels, Belgium

[b] Trilateral Research and Consulting, London, UK

Version of record first published: 15 Feb 2013.

To cite this article: Paul de Hert , Vagelis Papakonstantinou , David Wright & Serge Gutwirth (2013): The proposed Regulation and the construction of a principles-driven system for individual data protection, Innovation: The European Journal of Social Science Research, DOI:10.1080/13511610.2013.734047

To link to this article: http://dx.doi.org/10.1080/13511610.2013.734047

Innovation – The European Journal of Social Science Research
2013, 1–12, iFirst article

COMMENT

The proposed Regulation and the construction of a principles-driven system for individual data protection

Paul de Hert[a]*, Vagelis Papakonstantinou[a], David Wright[b] and Serge Gutwirth[a]

[a]*Vrije Universiteit Brussels – Tilburg University (TILT), Brussels, Belgium;* [b]*Trilateral Research and Consulting, London, UK*

(*Received 14 March 2012; final version received 21 September 2012*)

The overhaul of the EU data protection regime is a welcome development for various reasons: the 1995 Directive is largely outdated and cumbersome within an Internet (indeed, Web 2.0) environment. The 2008 Framework Decision is a practically unenforceable instrument, and even harmful in its weakness in protecting personal data. The Commission's proposed Regulation and Directive intended to replace it to improve the data protection afforded to individuals in their respective fields of application across the EU today. This paper considers some of the principles, some new, some old, that underpin the proposed new data protection framework, which was released on 25 January 2012. We offer an analysis of the key principles of lawfulness of the processing, access to justice, transparency and accountability – principles intended to be all-encompassing, abstract and omnipresent. Some of the above principles may appear to be new, but such is not necessarily the case. For instance, the principle of lawfulness is central in the current 1995 Directive, but it reappears in an amended form in the proposed EU data protection framework. On the other hand, the principle of accountability is an addition to the list that will need to prove its value in practice. Regardless of the outcome of the EU data protection framework amendment process and the ultimate wording of the instruments that compose it, the application and visibility of these principles ought to remain unaffected.

Keywords: data protection; 2012 amendment of the EU data protection framework; Draft General Data Protection Regulation; Draft Police and Criminal Justice Data Protection Directive

Introduction

The Commission initiated the process of amending the EU data protection framework in 2009. After public consultations were held, the Commission released a Communication in late 2010 (European Commission 2010). Subsequently, all major participants in the process published their views (Article 29 Data Protection Working Party 2011; European Council 2011; European Data Protection Supervisor 2011; European Parliament 2011a). Altogether, this documentation creates the institutional and theoretical environment that led to the Commission draft proposals released on 25 January 2012: the proposed General Data Protection Regulation (European Commission 2012b) and the proposed Police and Criminal Justice Data Protection Directive (European Commission 2012a). The former is intended to replace the EU Data Protection Directive (European Parliament and the Council

*Corresponding author: Email: paul.de.hert@uvt.nl

ISSN 1351-1610 print/ISSN 1469-8412 online

http://dx.doi.org/10.1080/13511610.2013.734047
http://www.tandfonline.com

1995), a document that since its release in 1995 has been the basic reference text for data protection worldwide. The latter intends to replace a specific legal instrument, the 2008 Framework Decision on the processing of data relating to security and criminal justice (European Council 2008).

The Commission proposals for the amendment of the EU data protection framework are not only impressive in volume – both comprise no less than 155 articles (and 172 pages) – but also wide-reaching and ambitious in scope. The Regulation in particular is a detailed document, each provision of which invites discussion in terms of aims, effectiveness and proportionality.

Rather than giving a detailed analysis of the provisions of both texts, which are still drafts, we examine in this paper the principles underlying the proposed new data protection rules. These principles are intended to be all-encompassing, abstract and omnipresent through the amended EU data protection framework, regardless of whether in the proposed Regulation or in the Directive or elsewhere. To this end, an analysis of the principles of lawfulness of the processing, access to justice, transparency and accountability follows. Regardless of the outcome of the EU data protection framework amendment process and the ultimate wording of the instruments that compose it, the application and visibility of these principles ought to remain unaffected.

After presenting in brief the main changes brought by the Commission proposals to the EU data protection framework in effect today, we elaborate the principles of lawfulness of the processing, access to justice, transparency and accountability, and their ramifications for the EU data protection system in the analysis that follows.

Some of the above principles may appear to be new, but such is not necessarily the case. For instance, the principle of lawfulness (discussed below) is central in the current 1995 Directive, but it reappears in an amended form in the proposed EU data protection framework. On the other hand, the principle of accountability (discussed below) is an addition to the list that will need to prove its value in practice.

A brief analysis of some of the new proposed data protection rights

One of the reasons for the change of the 1995 Directive through a Regulation lies in the lack of a sufficient harmonization level in data protection laws across the EU today. The 1995 Directive failed to create a uniform regulatory environment, in which all Member States would abide by (exactly) the same rules. As a rule, a Directive is not supposed to completely harmonize legal systems. Unlike a Regulation, some legal discretion is left to the Member States in its implementation. History has shown, however, that too much discretion was left in the hands of the Member States. Contemporary processing activities, which routinely transcend national borders, have helped to accentuate such disparities (notoriously, Google's Street View was received very differently among Member States). Because the creation of a single regulatory environment is deemed essential and because Member States evidently cannot be trusted to create such an environment through a Directive, the Commission has opted for a Regulation, an EU legal instrument that allows much more detailed and unifying (rather than harmonizing) regulation, which, once adopted, enables direct application into national laws (European Commission 2012b, 5).

In addition to unifying of data protection rules across the Member States, a primary task of the Regulation is to update the 1995 Directive's provisions into the contemporary personal data processing environment. The Directive was drafted at a

time when the Internet was little known. Evidently, the same applies to applications such as social networking websites, cloud computing and geo-location services. It is not, however, only a lack of technology updates that plagues the Directive's provisions: its personal data processing model has become out of phase in the meantime. In essence, the 1995 Directive assumed that a single, well-identifiable entity, named the "data controller", would take the initiative and control the circumstances of a single personal data processing operation. At best, such a data controller would be assisted, passively, by a "data processor". In this way, all processing operations could be singled out, and indeed catalogued into a registry held by the controlling mechanism (the Data Protection Authority). As is widely known, practically all of the above assumptions have been overturned in the contemporary processing environment.

Therefore, the proposed Regulation boldly updates the 1995 Directive provisions, reinforcing the mechanisms that seem to be working and deleting those that appear no longer connected to the state of the art. The list of information principles in the Directive that describes how processing should be carried out ("Principles relating to data quality" and "Principles regarding confidentiality and security of processing") continues to hold a central place in personal data processing (in Article 5); to the list is added, under the same Article, the data minimization principle and the "establishment of a comprehensive responsibility and liability of the controller" (European Commission 2012b, 8).

The same is the case with the set of individual data protection rights: the rights to information, access to one's personal data and rectification are substantially reinforced, in order to deal with contemporary complexity (in Articles 14, 15 and 16 respectively). Data exports to third countries continue to require the "adequacy" criterion (in Article 41). On the other hand, the new Regulation will abolish the notification system; it is to be replaced by data controller accountability, a system of prior notifications whenever needed, data protection impact assessments and the establishment of data protection officers in organizations with more than 250 employees.[1]

Replacing the Directive alone would have been a formidable task. However, the Commission chose to go much further than that: in addition to the above, it introduced a series of novelties that have already attracted the public's attention and, if ultimately adopted, are expected to play a significant role in the renewed EU data protection framework.

The introduction of a "right to be forgotten", in Article 17, is probably the best example from this point of view. The Commission decided to include in its proposal an individual's right to order that his or her data on the Internet be deleted, in spite of the strong criticism both from a practical (i.e. its applicability) and a theoretical (i.e. its relation to freedom of expression) perspective. Another novelty is the introduction of mandatory data protection impact assessments, in Article 33, following the example of environmental policy and law. Intended to precede risky processing operations, data protection impact assessments are expected to form yet another tool for the better monitoring of the Regulation's application. Finally, the same applies to "privacy-by-design" implementations (Article 23): by expressly acknowledging them in the proposed Regulation text, the Commission demonstrated that it considers such technical means important parts of the EU data protection model.

The other component in the Commission's proposed overhaul of the data protection framework is a new Police and Criminal Justice Data Protection Directive.

It might appear less ambitious in comparison to the Regulation; however, if ultimately adopted, it will bring substantial improvements in individual rights protection in a field where such progress ought not be taken for granted. The Directive would replace the 2008 Framework Decision. It would make a significant contribution to individual data protection, because the 2008 Framework Decision is ill-suited to serve its declared purposes, that is, to regulate security-related personal data processing in the EU. Such processing increased exponentially in importance after 9/11 and subsequent terrorist attacks in European capitals. However, data protection regulation never really caught up with processing developments in this field. Rather than establishing a coherent regulatory system (the 1995 Directive did not apply, as stated in its Article 3), specific sectors went on by themselves to establish their own data protection regime (for instance, the Schengen Information System, Europol, Eurojust, bilateral Passenger Name Records (PNR) Agreements, etc.). The 2008 Framework Decision was a latecomer in the field that, instead of providing the long-awaited principles and rules by which all other sector-specific instruments should abide, limited its scope to cross-border processing only. In addition, it provides for exemptions from practically every single fair information principle, while also failing to introduce a supervisory or coordinating body at EU level.

The proposed Directive broadly follows the Regulation's structure and wording. Its scope (Article 2) covers domestic data processing as well; the fair information principles and the individual rights of information, access to data and rectification are acknowledged (in Articles 4, 11, 12 and 15, respectively), while space for exemptions is kept at a minimum. On the other hand, differentiations are noted where the Commission considered that security-related processing deserves specialized treatment: data quality requirements are more relaxed (see, for instance, Article 6); profiling is allowed (in Article 9); and other personal data processing instruments relating to the area of freedom, security and justice remain unaffected by its provisions (see Article 59).

The principle of lawfulness: quality and legitimacy as conjunctive requirements

Let us now turn to a discussion of the proposed legal instruments and their underlying basic principles. The principle of lawfulness ought to be listed first among them. We therefore start with a complex message about the principle that processing should show a certain quality and the principle that processing needs to have a solid legal starting point: either consent, or a legal mandate, or any other recognized or legitimate starting point. Together both requirements – quality and legitimacy – create a lawful basis.

Articles 6 and 7 of the 1995 Directive prescribe the conditions under which personal data processing becomes lawful in the EU: the former pertains to the "principles relating to data quality" and the latter to the "criteria for making data processing legitimate". However, no clear guidance is found in the text of the 1995 Directive regarding the relationship between them. In practice, only Recital 30 provides some assistance to this end: Articles 6 and 7 ought to be read conjunctively – both the data quality conditions and the processing legitimacy grounds should concur in order for a specific processing to be lawful. This is of paramount importance to personal data protection. Any processing operation cannot be based on only one of these Articles: a processing operation adhering to all the "principles relating to data quality" may be found unlawful if it is not based on individual

consent or the other legal bases laid down in Article 7 of the 1995 Directive. Or a processing operation that is indeed based on individual consent or on any other of the legal bases of Article 7 may be found unlawful if it is not conducted according to all "principles relating to data quality" of Article 6. Application here is conjunctive and not selective.[2]

Nevertheless, the 1995 Directive's lack of a clear and straightforward connection between Articles 6 and 7 allowed data processors to adopt at times an opportunistic approach, whereby they could – erroneously from our point of view – argue that they could choose to apply only Article 7 or only Article 6 in order to justify the legitimacy of their processing (Knyrim and Trieb 2011).

The proposed Regulation does not have an explicit and unequivocal provision requiring both Articles (now, 5 and 6) to apply to any and all personal data processing operation in order for it to be lawful. In addition, the helpful wording of the 1995 Directive Recital 30 has now been replaced, further undermining the above interpretation.[3] Consequently, opportunistic data processor approaches may continue, if not increase, once the new regulatory framework comes into place. Such a change shall gravely worsen individual data protection. The lack of clear guidance as to the exact conditions for the principle of lawfulness to apply to personal data processing is a significant omission by the Commission, which needs to be addressed in the future.

The principle of access to justice and the creation of a "closest to the home" individual redress right

Let us now turn to a second principle: the data subject needs to have good access to the legal system to challenge processing practices. Within a globalized international environment permeated by the Internet, the issue of local jurisdiction appears impossible to resolve. Effectively, it exceeds the data protection boundaries, being ultimately relevant to all fields of law that enable any level of international interaction at individual level without the intervention of intermediaries. However, this issue is increasingly pressing for data protection for two reasons. First, it affects individuals directly: an individual residing in a Member State may have to support her case on the infringement of her data protection rights outside her own country, or even outside the EU itself – an expensive, complex and time-consuming undertaking that is normally not accessible to the majority of the persons concerned. Second, it is sensitive to differences between intra-EU data protection models, impeding adherence to data protection regulations by data controllers with multiple places of residence. Exactly this shortcoming of the 1995 Directive led to the Commission's proposal for a change of instrument in the form of a Regulation.

The distinguishing criteria for the applicable law employed by the 1995 Directive refer primarily to the location of the data controller and, alternatively, to the location of its equipment.[4] The general rule sets out that the Member State's Data Protection Act applicable each time is the one of the residence of the data controller concerned. If the data controller is not established on EU territory, then a specific Member State Data Protection Act may still apply, if the data controller uses equipment located within its territory. The criterion is therefore of a "locality" nature. As such, however, this criterion has proven of limited practical use to individuals, because, even if they are able to establish the whereabouts of either the data controller or its equipment, they will ultimately be forced to get involved in expensive and time-consuming litigation outside their own country of residence.[5]

Nor is the 1995 Directive accommodating with regard to multi-national data controllers' needs. Article 4.1 states that, "when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable". This task has proven quite difficult to accomplish over the years, owing to a lack of harmonization among Member States.

A bold, user-centric approach is admittedly adopted in the text of the proposed Regulation.[6] Abandoning the "chase for the server", a task further complicated in cloud computing and "software-as-a-service" environments (European Data Protection Supervisor 2010), the Regulation is intended to apply to processing of personal data executed not only by data controllers or processors within the EU but also by processors established in third countries, where the processing activities are related to "the offering of goods or services" to data subjects residing in the EU or "serve to monitor their behaviour" (Article 3.2).[7] Whether this provision is kept in the Regulation's final wording remains to be seen, particularly given that it appears to regulate the whole of the Internet (and, perhaps indirectly, the whole of the world).[8]

The user-centric approach is further reinforced by a series of new powers granted to national data protection authorities. Data controllers not established in the Union are expected to appoint representatives, who are obliged to cooperate with the local data protection authorities (Article 29). Supervisory authorities carry a mandate to cooperate and coordinate among themselves, providing, among other things, mutual assistance (Article 55) and carrying our joint operations (Article 56), in order to warrant to individuals an increased level of protection in the contemporary cross-border processing environment.

Nevertheless, resolving jurisdictional issues does not necessarily mean improving individuals' access to justice as well. This is why the draft Regulation, in its Chapter VIII, grants individuals the right to lodge a complaint against a controller or a processor either before the courts of the Member State where the controller or processor has an establishment or before the courts of the Member State where the data subject has its habitual residence.[9] This, "closest to the home" individual redress right, together with the principle of accountability discussed in the next section, is expected to assist individuals to effectively exercise their right to data protection.

The principle of transparency

The principle of transparency is particularly important in the data protection field. Processing operations do not take place in public, nor are their results felt immediately by the individuals concerned, in order for them to respond accordingly. On the contrary, the processing of personal data takes place behind closed doors, or rather within automated systems, without the individuals whose data are being processed being present or even aware that such processing takes place. The knowledge generated about an individual is very often not accessible to her, nor any information about how it was produced. In addition, the results of such processing in the majority of cases do not lead to direct action, positive or negative, towards the individuals concerned, but are rather stored in computer systems for future use. In the real world, individuals come across decisions that affect them (for instance, rejection of a loan or insurance policy, failure to get a job, failure to enter a country) yet are unaware of the automated processing operations the results of which have been used to formulate such decisions. The task of safeguarding their rights is

virtually impossible: individuals do not know that their data have been processed unless they are faced with a (negative) decision against them. Only then do they have reason to start inquiring how or why a decision was made. They need all the help they can get to learn what happened.

The principle of transparency is therefore of paramount importance for the creation of an effective data protection regulatory framework: it fosters a personal data processing environment of trust and enables any interested party to enforce effectively data protection rights and obligations. However, its effect may only be fully appreciated when it operates at multiple levels.[10] In particular, the principle of transparency needs to apply to data controllers and data processors alike as well as to the processing operations themselves. It also needs to apply to the data protection enforcement mechanism. An enforcement mechanism must be open and transparent to citizens and to any third party with an interest in inquiring about its operation and effectiveness.

The principle of transparency is acknowledged in the text of the 1995 Directive, albeit not expressly. Instead, its established mechanisms serve its causes indirectly. The notification system is such an example. Transparency within the 1995 Directive framework may also be achieved, from the data subject's point of view, through exercising rights to information and access. It may also be achieved through the obligation of national data protection authorities to submit formal annual reports.

The proposed Regulation places the principle of transparency at its epicenter. With regard to its meaning in the data protection context, "the principle of transparency requires that any information, both of the public and of the data subject should be easily accessible and easy to understand, and that clear and plain language is used" (European Commission 2012b, Recital 39). A new relevant principle is expressly introduced in its list of Fair Information Principles, complementing the fairness and lawfulness of the processing principle: "personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject". Accordingly, data controllers carry an explicit obligation: Article 11 introduces the obligation for "transparent information and communication".[11] All aforementioned transparency instances in the text of the 1995 Directive (apart from the notification system) are maintained in the draft Regulation.

The proposed Directive on police and justice processing does not seem to follow the Regulation's example with regard to the principle of transparency, restricting it (in fact, the only relevant reference may be found in its Article 10) perhaps according to perceived specialized security-related processing needs. From this point of view, notwithstanding the plausibility of a distinction between the two types of processing, individuals may be surprised when they discover that safeguards afforded to them in general personal data processing are not even remotely applicable in security-related circumstances. Solutions may be sought in trusted third party systems that would provide the controls and checks upon request of a data subject, without passing her substantial information about the processing itself. Data Protection Authorities could act as such trusted third parties.

The principle of accountability: the revolutionary newcomer

The introduction of a principle of accountability for data controllers in the personal data processing context (European Parliament 2011b) is by no means a new idea in the field. Discussions from a legal point of view date as far back as 2009 (Article 29

Data Protection Working Party 2010a, 2011). Its explicit appearance in the text of the draft Regulation should come as no surprise either to data protection proponents or data controllers.

In broad terms, a principle of accountability would place upon data controllers the burden of implementing within their organizations specific measures in order to ensure that data protection requirements are met. Such measures could include anything from the appointment of a data protection officer to implementing data protection impact assessments or employing a privacy-by-design system architecture (European Commission 2010; Article 29 Data Protection Working Party 2011). The Commission, in its Communication on the amendment of the EU data protection framework, perhaps worryingly, connected an introduction of a principle of accountability with a reduction in the data controllers' "administrative formalities".[12] It is exactly at this point where a major concern before the introduction of the draft Regulation lay: what exactly would be the added value of introducing a general principle of accountability into the overall, sound, principles-based environment of the 1995 Directive? Data controllers are anyway responsible for observing the data protection rules. Is a principle of accountability to be perceived as an alternative to certain requirements for compliance with rules? If it means the abolition of administrative procedures regarded as a bureaucratic burden by data controllers, would it not at the same time compromise the level of protection afforded to individuals?

Various views have been expressed on this issue. The principle of accountability would need to address difficult questions, such as how to reconcile the need for specificity with a general nature principle or how to resolve the issue of scalability or proportionality. In other words, which criteria shall decide the adequacy of measures implemented by data controllers?[13] It has also been suggested that the added value of a general principle of accountability lies in the fact that it could function as a general obligation to demonstrate results, while leaving freedom to data controllers as to the means they employ (Hijmans 2011).

The wording of the proposed Regulation attempts to alleviate these data protection concerns. Article 22 "takes account of the debate on a 'principle of accountability' and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance" (European Commission 2012b, para. 3.4.4). As such, the principle of accountability in the draft Regulation indeed introduces a results-oriented criterion: data controllers are free to decide which policies and measures to introduce in order to achieve verifiable results: "the controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation" (Article 22.1). However, the draft Regulation does provide further guidance, in the form of minimum requirements for data controllers: these include keeping the required documentation, implementing data security measures, performing data protection impact assessments or prior consultations or designating a data protection officer. Their implementation may be externally audited. Altogether, these minimum requirements admittedly set rather high standards for data controllers.

We can see novelties in the proposed Regulation, such as privacy by design (in Article 23) or personal data breach notifications (in Article 31) in this same quid-pro-quo context. For example, data controllers win the abolition of the notification

system and other bureaucratic burdens but in return are expected to act responsibly. Practically, they are left alone to decide upon the circumstances of their personal data processing; unless they are audited and found lacking (or unless the Commission identifies a whole sector in need of intervention and decides to intervene), they are mostly left unhindered in their activities.[14]

Finally, an important consequence of the introduction of the principle of accountability into the data protection field is the reversal of the burden of proof in favor of individuals. Because personal data processing is customarily conducted behind closed doors and individuals only become aware of their data being processed whenever (adverse) results affect them, they are frequently unable to adequately prove their case in courts. Therefore, a reversal of the burden of proof obliges data controllers to demonstrate that they comply with the law, that the various legal prescriptions were applied faultlessly. The data subject does not have to demonstrate exactly where the processing, which they never witness, went wrong. This would substantially increase individual protection. This option would also be in line with fundamental case law by the European Court on Human Rights (2008): in effect, the Court has recognized the inability of an individual to prove his or her case before national courts but has concluded that "to place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the [data controller]'s record keeping at the material time".

The reversal of the burden of proof is not included in Article 22 of the draft Regulation but is found in various other provisions in its text (for instance, in Articles 7, 12 or even 19). Altogether, particularly if combined with the potential severity of penalties and sanctions suggested in the proposed Regulation, their contribution to personal data protection is expected to be critical.

Conclusion

The overhaul of the EU data protection regime is a welcome development for various reasons: the 1995 Directive is largely outdated and cumbersome within an Internet (indeed, Web 2.0) environment. The 2008 Framework Decision is a practically unenforceable instrument, and even harmful in its weakness in protecting personal data. The Commission's proposed Regulation and Directive intended to replace them and improve data protection afforded to individuals in their respective fields of application across the EU today.

This, however, is most likely the only statement that would equally apply to both sets of regulatory texts under discussion.[15] Once it is agreed that the instruments in effect today are in dire need of replacement, and new rules have been released to this end, each process goes its own separate and distinct way. While the proposed Regulation in its current wording appears to make positive contributions to individual data protection (De Hert and Papakonstantinou 2012), the same cannot always be held for the proposed Directive. Practically, of the four identified system-guiding principles above, whose efficient implementation offers an increased level of data protection, two are completely missing from the text of the Directive (the principles of transparency and accountability) and one is more or less inapplicable (the principle of access to justice). Concerns about the Directive's proposed provisions are thus justified.

The above differentiation is probably the inevitable result of a distinction made at an earlier stage by the Commission: that general-purpose and security-related

personal data processing are and should be distinguished, each deserving separate rules and regulations. However, this distinction is artificial and impossible to apply in an increasingly interconnected, processing-intensive environment.[16] Also, one can challenge the assumption that security-processing of personal data merits a substantially and fundamentally different treatment than general-purpose processing.[17]

The construction of a principles-driven system for individual data protection is the obvious option in view of contemporary data processing complexity. Personal data processing has become an economic, social and political phenomenon, whose exact circumstances are in constant flux. Attempting to predict, in order to regulate, its future forms or regulate in detail its contemporary appearances is a futile law-making pursuit. Instead, encompassing principles that remain broad in scope and technological specifications could provide the necessary guidance as to the applicable rules and regulations each time a processing operation appears to transcend existing models and schemes. To this end, the principles of lawfulness of processing, access to justice, transparency and accountability constitute the bases upon which the new EU data protection framework needs to build.

Notes

1. Admittedly, however, this is a considerable step backwards for those Member States that already have rules requiring significantly lower numbers.
2. This has important drawbacks with regards to the role of the data subject's consent in data protection. If one takes seriously the interplay between Article 6 and 7 of the 1995 Directive, it is not clear at all – in the general rules, and thus not for sensitive data – when a consent is really needed, and how it can contribute to "lawfulness". Consent is always additional, and thus per se superfluous. Hence there is no "principle of consent" in data protection and it should be avoided that consent be (ab)used for legitimizing processings that do not meet the other conditions spelled out in Article 6 and 7 (Gutwirth 2012).
3. The same appears to be the case with the proposed Justice and Police Directive (the respective Articles are 4 and 7).
4. See its Article 4. The Article 29 Working Party (2010b) made concrete recommendations for the amendments required to further enforce the relevant Directive provisions; its suggestions seem to have been adopted (European Commission 2010, section 2.2.3).
5. See European Commission (2010, section 2.2.3).
6. The Article 29 Working Party (2002) has already attempted to introduce similarly protective criteria since 2002, admittedly adopting a rather creative reasoning (see Moerel 2011).
7. See also the draft Regulation's Article 22, and on "national targeting", see Article 29 Data Protection Working Party (2010b, p. 31). On the other hand, the proposed Directive contains no extra-territorial effect.
8. This option may not be as burdensome, or even unrealistic, as one might imagine. When data controllers are powerful multinational organizations, as is often the case (for instance, search engines, social network websites, Web 2.0 providers), they can evidently cope with the costs of international litigation much more easily than individuals. In the same context, when "national targeting" may be established (for instance, web pages of country-specific interest or translated into the local language), then it is only reasonable that sales within such territory also include some (litigation) risks. Ultimately, if service providers are unwilling to undertake the risk of international litigation, they may very well refuse to provide services to individuals trying to connect from third countries (through their IP addresses); after all, this is a business policy frequently implemented in order to maximize international profits or to control international distribution channels and it would therefore be feasible for it to expand in order to minimize international exposure as well.

9. This option does not seem to be available to individuals in the proposed Directive.
10. The principle of transparency discussed here is broader than the "increasing transparency for data subjects" analysis included in the Commission Communication (section 2.1.2), in that the principle elaborated here is intended to operate at multiple levels, and addresses all data protection participants, rather than placing specific obligations upon data controllers only (thus, expanding the individual right to information).
11. As expressly inspired by the Madrid Resolution on international standards on the protection of personal data and privacy (European Commission 2012b, para. 3.4).
12. "This [principle of accountability] would not aim to increase the administrative burden on data controllers, since such measures would rather focus on establishing safeguards and mechanisms which make data protection compliance more effective while at the same time reducing and simplifying certain administrative formalities, such as notifications" (section 2.2.4).
13. A point favored by the Council (Győző 2011).
14. The proposed Directive does not appear to acknowledge application of a principle of accountability in the security processing field.
15. See also the European Data Protection Supervisor (2012b), in which the lack of comprehensiveness of the proposed regulatory framework is identified as its main weakness.
16. Distinguishing in practice between commercial and security personal data processing is extremely difficult. Apart from clear-cut cases whereby, for instance, data is collected by the police and kept in its systems, or data collected by commercial data controllers in the course of their duties may be used by law enforcement agencies and vice versa (see, for instance, Article 60 of the proposed Directive), case law provides little assistance to this end: although PNR processing was ultimately considered security-related, electronic communications processing was considered commercial processing (on PNR-related processing, which was found to be security-related in spite of the fact that data are collected by airline carriers for commercial purposes; see, for instance, Papakonstantinou and de Hert 2009). On the other hand, the retention of telecommunications data, collected by telecommunications providers for commercial purposes, has been judged as commercial processing (as established by the European Court of Justice in its Case C-301/06, Ireland v. Parliament and Council).
17. See, for instance, the EDPS Press Release on the proposed EU data protection framework (European Data Protection Supervisor 2012a).

References

Article 29 Data Protection Working Party. 2002. *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by non-EU Based Websites*, WP 56. Brussels, May 30.

Article 29 Data Protection Working Party. 2010a. *Opinion 3/2010 on the Principle of Accountability*, WP 173. Brussels, July 13.

Article 29 Data Protection Working Party. 2010b. *Opinion 8/2010 on Applicable Law*, WP 179. Brussels, December 16.

Article 29 Data Protection Working Party. 2011. *Letter to Vice-President Reading Regarding the Article 29 Data Protection Working Party's Reaction to the Commission Communication, "A Comprehensive Approach to Personal Data Protection in the EU"*. Brussels, January 14.

De Hert, P., and V. Papakonstantinou. 2012. "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals." *Computer Law and Security Review* 28 (2): 1–13.

European Commission. 2010. *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Comprehensive Approach on Personal Data Protection in the European Union*, COM(2010) 609 final. Brussels: European Commission, November 4.

European Commission. 2012a. *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution*

of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM(2012) 10 final. Brussels: European Commission.

European Commission. 2012b. *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. Brussels: European Commission.

European Council. 2008. *Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters*. Brussels: European Council.

European Council. 2011. *Conclusions on the Communication from the Commission to the European Parliament and the Council – A Comprehensive Approach on Personal Data Protection in the European Union, 3071st Justice and Home Affairs Council Meeting*. Brussels: European Council, February 24 and 25.

European Court on Human Rights. 2008. *K.U. vs. Finland*, Judgment of 2 December.

European Data Protection Supervisor. 2010. "*Data Protection and Cloud Computing under EU law*", Third European Cyber Security Awareness Day. Brussels: European Parliament, April 13.

European Data Protection Supervisor. 2011. *Opinion on the Communication from the Commission on "A Comprehensive Approach on Personal Data Protection in the European Union*." Brussels: European Data Protection Supervisor, January 14.

European Data Protection Supervisor. 2012a. *EDPS Welcomes a "Huge Step Forward for Data Protection in Europe", but Regrets Inadequate Rules for the Police and Justice Area*, EDPS/02/12. Brussels: European Data Protection Supervisor, January 25.

European Data Protection Supervisor. 2012b. *Opinion on the Data Protection Reform Package*. Brussels: European Data Protection Supervisor, March 7.

European Parliament. 2011a. *Committee on Civil Liberties, Justice and Home Affairs, Working Document (1 and 2) on a Comprehensive Approach on Personal Data Protection in the European Union*. Brussels: European Parliament, March 15.

European Parliament. 2011b. *Towards a New EU Legal Framework for Data Protection and Privacy, Committee on Civil Liberties, Justice and Home Affairs*. Brussels: European Parliament.

European Parliament and the Council. 1995. *Directive 95/46/EC 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*. Brussels: European Parliament and the Council. Accessed April 14 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Gutwirth, S. 2012. "Short Statement about the Role of Consent in the European Data Protection Directive." In: *The Selected Works of Serge Gutwirth*. Accessed April 14. http://works.bepress.com/serge_gutwirth/80

Győző, S. E. 2011. "New Principles – in the Light of the Discussions within the Council Conclusions on the Commission's Communication." Presentation to the International Data Protection Conference, Budapest, June 16 and 17.

Hijmans, H. 2011. "Principles of Data Protection: Renovation Needed?" Presentation to the International Data Protection Conference, Budapest, June 16 and 17.

Knyrim, R., and G. Trieb. 2011. "Smart Metering under EU Data Protection Law." *International Data Privacy Law* 1 (2): 121–128.

Moerel, L. 2011. "The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?" *International Data Privacy Law* 1 (1): 28–46.

Papakonstantinou, V., and P. De Hert. 2009. "The PNR Agreement and Transatlantic anti-Terrorism co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic." *Common Market Law Review* 46: 885–919.