BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 1 • N° 3 • OCTOBER 2015

Towards efficient cooperation between supervisory authorities in the area of data privacy law[1]

by Dariusz Kloza[2], Antonella Galetta[3]

Abstract

As research conducted in the framework of the PHAEDRA project (Improving Practical and Helpful cooperAtion betweEn Data Protection Authorities, 2013-2015) demonstrated, numerous cross-jurisdictional cooperation initiatives in the area of data privacy have flourished in the recent decades at bilateral, regional, supranational and international levels. However, it was also determined that these initiatives are still too immature to reach their final aim, i.e. the efficient protection of data privacy in matters producing implications in more than one jurisdiction. Therefore, this contribution discusses how to make such cooperation more efficient and how this goal could be achieved. A set of 23 legal and practical recommendations that might help both policy-makers and supervisory authorities overcome contemporary inefficiencies are proposed, including a modest action plan to that end. As a conclusion, a line is drawn between binding and non-binding types of cooperation.

Keywords: privacy, personal data protection, data privacy, data protection authorities, cooperation, enforcement, General Data Protection Regulation

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html

This version is for academic use only.

This working paper is a reprint of: Kloza Dariusz and Galetta Antonella (2015) "Towards efficient cooperation between supervisory authorities in the area of data privacy law", in De Hert Paul, Kloza Dariusz and Makowski Paweł (eds.) Enforcing privacy: lessons from current implementations and perspectives for the future, Wydawnictwo Sejmowe, Warszawa, pp. 77-108.
http://www.phaedra-project.eu/wp-content/uploads/phaedra1_enforcing_privacy_final.pdf

Disclaimer

1. Introduction

There is already a growing consensus in academic literature as well as amongst policy-makers that efficient cross-jurisdictional cooperation among national and/or regional supervisory authorities in the field of data privacy is indispensable in order to ensure adequate protection of (informational) privacy. It is further agreed that within a wide range of cooperation types and activities, it is the enforcement cooperation that is rather of paramount importance (e.g. Raab 2010; Raab 2011; Kloza, Mościbroda, and Boulet 2013; Kloza and Mościbroda 2014; Wright and De Hert 2015).

As the PHAEDRA research project has demonstrated,[4] numerous cross-jurisdictional cooperation initiatives in the area of data privacy have proliferated in the recent decades at bilateral, regional, supranational and international levels, although achieving thus far only moderate success. To put it simply, the existing mechanisms are still too immature to reach their final aim, i.e. the efficient protection of data privacy in matters producing implications in more than one jurisdiction. The cooperation process nowadays faces numerous barriers, both of legal (e.g. capacity, procedures, sharing information) and practical nature (e.g. resources, technical tools, languages, sharing costs), thus rendering it ineffective at best and at worst impossible. As a result, it is a fair contention that both supervisory authorities and policy-makers have realised the problem and thus committed themselves to achieve greater efficiency of such cooperation.[5] Therefore, it is not surprising that the quest for efficient cooperation among supervisory authorities has become one of the core aims of both European reforms of data protection frameworks, i.e. the European Union (EU)[6] and the Council of Europe (CoE).[7] In parallel, debates in academic circles proliferated and the PHAEDRA research project is a good example thereof.

The need for improving cooperation to achieve efficiency is not disputed and debates about how to shape efficient cooperation have not come to a conclusion. This chapter aims to bring its own modest conclusion to the table. It builds on a previous contribution of similar nature, namely (Kloza and Mościbroda 2014), in which lessons for the enforcement cooperation of supervisory authorities in the area of data privacy law were drawn from analogous cooperation in the field of European competition law. Going beyond mere enforcement cooperation, we will propose 23 legal and practical recommendations that might help overcome contemporary inefficiencies.

---

[1] We thank Michał Boni, Paul De Hert, Ian Lloyd, Paul Quinn, Dan Jerker B. Svantesson and Wojciech Wiewiórowski for their comments on an early draft of this chapter.

[2] Dariusz Kloza is researcher at Vrije Universiteit Brussel (VUB), Research Group on Law, Science, Technology and Society (LSTS) and at VUB's Institute for European Studies (IES), dariusz.kloza@vub.ac.be.

[3] Antonella Galetta is researcher at VUB-LSTS, antonella.galetta@vub.ac.be.

[4] This chapter is based on the research project PHAEDRA (*Improving Practical and Helpful cooperation between Data Protection Authorities*; 2013-2015), co-funded by the European Union under its Fundamental Rights and Citizenship Programme; http://www.phaedra-project.eu. The research consortium is composed by the Vrije Universiteit Brussel (Belgium; coordinator), Trilateral Research and Consulting LLP (UK), Generalny Inspektor Ochrony Danych Osobowych (Polish DPA) and Universidad Jaume I (Spain). The contents are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

[5] Most recently, 36th International Conference of Data Protection and Privacy Commissioners (ICDPPC, 2014) has adopted another resolution, fifth in a row, on enforcement cooperation. Cf. http://www.privacyconference2014.org/media/16605/Resolution-International-cooperation.pdf. At a regional level, European Data Protection Authorities' Conference ("Spring Conference"; 2015), in a resolution on "Meeting data protection expectations in the digital future", called for ensuring that "the funding of Data Protection Authorities is sufficient to meet the ever increasing demands on them", including "the need for mutual cooperation" (§ 1). Cf. https://ico.org.uk/media/about-the-ico/events-and-webinars/1431804/ecdpa2015-draft-resolution-meeting-data-protection-expectations-in-the-digital-future-final-adopted.pdf.

[6] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Brussels, 25 January 2012, COM(2012)11 final (*hereinafter*: GDPR). Whenever a reference is made to the EU reform, we refer to the original text of the proposal as – at the time of writing (July 2015) – it is still being negotiated.

[7] Council of Europe, *Modernisation of Convention 108*, Strasbourg, 29 November 2012, T-PD(2012)4Rev3_en.

They are addressed, respectively, to policy-makers, i.e. regulators developing framework(s) and arrangement(s) for cooperation, and to supervisory authorities themselves, suggesting actions they could undertake; although this distinction is not often clear-cut. Having provided an overview of the state of the art of cooperation in data privacy law (Section 2), we will briefly introduce the core elements that make the functioning of enforcement cooperation in competition law efficient (Section 3). Based on these findings, our main recommendations will be elaborated in Section 4, which also suggests an action plan concerning the development of efficient cooperation in data privacy law (Section 4.3). Our analysis aims to fuel discussion and, in particular, to inform the on-going reforms of European data protection frameworks. These recommendations are not exhaustive in nature and – as the PHAEDRA project continues till January 2017 – remain open for further discussion.

The relevant experience of both authors of the present chapter results from their involvement in the work of the PHAEDRA project.[8] The project focused on improving *practical* cooperation and coordination between supervisory authorities in the area of data privacy law around the world, with a special focus on the *enforcement* of these laws. Having recognized the critical need for more efficiency is such cooperation, the project analysed the state-of-the-art, identified obstacles (both legal and extra-legal) and areas for improvement and – finally – advised policy-makes and authorities themselves in that regard. The research has been fuelled by a high level of interaction with the concerned authorities via, among others, interviews, surveys and workshops.

Some preliminary clarifications, however, are needed before digging into the topic of this chapter. First, our analysis is targeted towards an *efficient* cooperation amongst supervisory authorities, instead of an *effective* one. The expression "effective cooperation" is recurrent in data privacy law,[9] effectiveness being the possibility or capability of producing a result.[10] We rather argue for such cooperation to be efficient, efficiency being the possibility or capability of "functioning or producing effectively and with the least waste of effort".[11] Thus, we claim that cooperation initiatives should reach certain objectives but with the smallest possible waste of financial, human and technical resources, which are critical to supervisory authorities (European Union Agency for Fundamental Rights 2010). In so doing, we aim to strive for the highest possible cooperation standard in data privacy law. Second, following Kuner et al., we have consciously selected the the term "data privacy" – embracing in particular the European understanding of "personal data protection" and the Anglo-Saxon one of "informational privacy" – in order to "avoid terminology that might seem focused too much on a particular legal system" (Kuner et al. 2014). Third, for similar reasons, we have selected the term "supervisory authority"[12] to indicate relevant public bodies tasked with the governance of data privacy in a given jurisdiction. The term we use here comprises data protection authorities (DPAs), privacy commissioners (PC), privacy enforcing authorities (PEAs) (Stewart 2013) and – a novelty in our "dictionary" – privacy enforcing agencies (Bygrave 2014).[13] Only some of these bodies are independent regulatory authorities, while others may be public bodies tasked *prima facie* with other issues, but dealing with data privacy too. We opt for this all-encompassing approach as independence is not always a requirement for cooperation in data privacy law and such cooperation may involve authorities at various

[8] *Supra note* 4.

[9] Cf. e.g. Recital 11 as well as Articles 45–46, 55 and 66(1)(e) GDPR.

[10] Collins English Dictionary, http://www.collinsdictionary.com.

[11] *Ibid.*

[12] Actually, the 1995 Data Protection Directive, in Article 28, uses this term, but gives it a particular definition, from which we detach here. 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, OJ L 281, 23.11.1995, pp. 31–50.

[13] There exist also "specialist privacy tribunals" tasked with enforcing privacy laws, e.g. so tasked is New Zealand's Human Rights Review Tribunal, but these bodies are rather of a judicial nature. Cf. Sect. 82ff of Privacy Act 1993, as amended. http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

levels. Still, we are aware that supervisory authorities are not endowed with the same functions and powers (Bennett and Raab 2006) as well as resources, which is often reflected in their willingness and ability to cooperate as well as in the scope thereof. (We are also aware that not only public bodies might be involved in the protection of data privacy, e.g. NGOs, but these do not focus on enforcement and thus fall outside the term "supervisory authorities".) Fourth, by a "cross-jurisdictional data privacy violation" we refer to a breach of data privacy laws producing effects or implications in more than one jurisdiction. Finally, by "cooperation" we mean a spectre of activities undertaken together by supervisory authorities in fulfilling their functions and duties. This cooperation is not of a uniform nature and can range from "soft" forms, such as policy shaping, exchange of good practice, training, study visits, research or education, to "hard" ones, like enforcement of data privacy laws in cross-jurisdictional cases. For (Baggaley 2014), these latter forms of cooperation can vary from: (1) sharing of non-confidential information, to (2) coordinated compliance activities, to (3) sharing confidential information, and to (4) formal enforcement cooperation (Fig. 1).

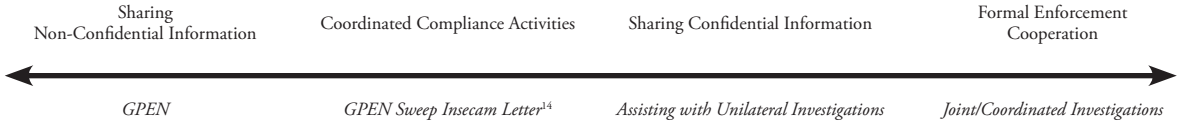

Figure 1. The enforcement cooperation spectrum

2. Why do we need cooperation in data privacy law to be more efficient? The state of the art

But why do we need cooperation in a first place? On the one hand, the main reason has to do with the growing importance of information in the contemporary, globalised world; on the other, it pertains to the risks to the individual and the society this growth of importance poses. It is often argued that "data is the new oil", that is to say, "data in the 21st century is like oil in the 18th century: an immensely, untapped valuable asset" (Toonders 2014). These days, worldwide, regional, national and local economies as well as public and state security practices are fuelled by information. However beneficial this phenomenon is, drawbacks emerge. Lots of information that relate in one way or another to an individual almost always "travels" through national borders. The constant progress of technology brings every day new means and possibilities for the processing of personal information; yet these novelties are not always entirely beneficial for the individual concerned. All these phenomena have resulted in the elevation of risks and thus threaten the protection of the fundamental rights to privacy and personal data protection, recognised by the majority of Western liberal democracies. This requires adequate responses to prevent such risks and sanction corresponding violations, should they occur. As it is the supervisory authorities that are predominantly tasked with the day-to-day protection of data privacy, on their shoulders lies the main burden of effective protection, also with cross-jurisdictional implications.

From the formal point of view, within the scope of data privacy laws, cooperation does often represent the sole means to effectively remedy data privacy violations. (Otherwise individuals would need to use other mechanisms, such as consumer law.) Speaking even more practically, a lack thereof usually entails a duplication of efforts in investigating and/or sanctioning violations, ultimately leading towards inconsistent enforcement. It follows that some of the duties performed by supervisory authorities – "by reason of the scale or effects" – might be better and more efficiently under-

[14] Cf. http://www.privacycommission.be/en/internet-privacy-sweep-2013.

taken jointly with their counterparts.[15]

However, data privacy law is very much built upon the interplay among data subjects, data controllers or processors and supervisory authorities. If follows that cooperation among supervisory authorities should not only be aimed at easing tasks and smoothing procedures, but also at strengthening data subject's rights and benefit – or at least not damage – data controllers and processors.

And why do we need to increase the efficiency of cooperation? The reasons are at least twofold, yet simple. First, the *status quo* does not entirely live up to the expectations vested therein. Although several arrangements and frameworks of cooperation are already put in place at various levels, and despite some successes in recent years,[16] we claim they are not yet as *effective* (not to even mention *efficient*) as they could or should be. Second, the multiplication of cooperation arrangements and frameworks, supplemented by the lack of coordination between them, only adds to their inefficiency. Barnard-Wills and Wright (2014), for example, have nicely captured the most of such complication: Fig. 2 maps the existing cooperation frameworks, showing the overlap between their memberships, namely:

1. Global Privacy Enhancement Network (GPEN),[17]
2. European Conference of Data Protection Authorities (ECDPA; "Spring Conference"),[18]
3. Article 29 Working Party,[19]
4. Asia-Pacific Privacy Authorities (APPA),[20]
5. Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement (APEC CPEA),[21]
6. APEC Cross-Border Privacy Rules (APEC CBPR),[22]
7. Association francophone des autorités de protection des données personnelles (AFAPDP),[23]
8. British, Irish and the Islands Data Protection Authorities (BI&TI).[24]

Still, the diagram illustrated at Fig. 2 is obviously not exhaustive. In fact, there are at least four additional cooperation frameworks that should be added, namely: (1) the framework created by the Council of Europe's Convention 108,[25] (2) the International Conference of Data Protection and Privacy Commissioners (ICDPPC),[26] (3) the International Working Group on Data Protection in Telecommunications (IWGDPT; 'the Berlin Group'),[27] (4) the Red Iberoamericana de Protec-

[15] Here we have been obviously inspired by the contents of the principle of subsidiarity spelled out in Article 5 TEU: "Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level".

[16] We have been particularly impressed by the efficiency of the Dutch-Canadian 2014-2015 investigation into Whatsapp. CPB, *Investigation into the processing of personal data for the 'whatsapp' mobile application by Whatsapp Inc., Z2011–00987, Report on the definitive findings*, The Hague, 15 January 2013, pp. 6–7, https://cbpweb.nl/sites/default/files/downloads/rapporten/rap_2013-whatsapp-cbp-definitieve-bevindingen-nl.pdf Office of the Privacy Commissioner of Canada, *Report of Findings Investigation into the personal information handling practices of WhatsApp Inc., PIPEDA Report of Findings #2013–001*, Ottawa, 15 January 2013, http://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp.

[17] Cf. http://www.privacyenforcement.net.

[18] For the 2015 edition, cf. http://eurospringconference.wordpress.com.

[19] Cf. http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

[20] Cf. http://www.appaforum.org.

[21] Cf. http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

[22] Cf. http://www.cbprs.org.

[23] Cf. http://www.afapdp.org.

[24] Rather informal.

[25] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108.

[26] For the upcoming 2015 edition (in October), cf. https://www.privacyconference2015.org.

[27] Cf. http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt.

ción de datos (RIPD)[28] and Central and Eastern Europe Data Protection Authorities (CEEDPA).[29] Furthermore, one must complete this picture by adding numerous bilateral arrangements between various supervisory authorities and/or their networks.

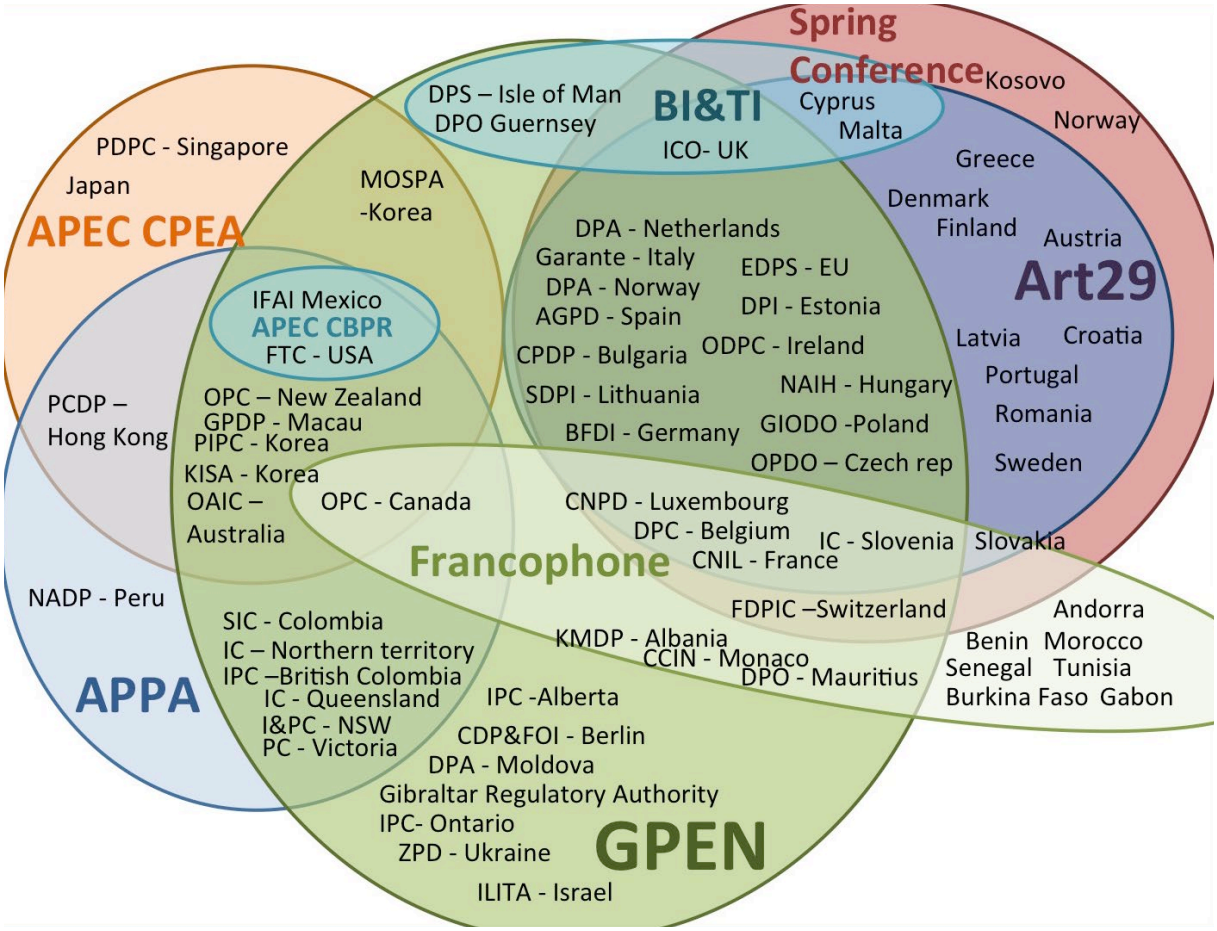

Figure 2. Key international cooperation mechanisms, showing the overlap between their memberships (Barnard-Wills and Wright 2014, 139)

3. Lessons from enforcement cooperation in European competition law

The analysis thus far leads us to the conclusion that cooperation among supervisory authorities in the area of data privacy law is still in its infancy and there is significant room for improvement. Hence, how would it be possible to make such cooperation more efficient? Our starting point would be to recall a few lessons learnt from *enforcement* cooperation in European competition law that would subsequently constitute a basis for a broader set of legal and practical recommendations.[30] *Enforcement* cooperation in competition law[31] shares a lot of similarities with its counterpart in data privacy law. First and foremost, globalization and developments in information and communications technologies (ICT) result in an increasing number of multi-jurisdictional cases and thus

[28] Cf. http://www.redipd.org.

[29] Cf. http://www.ceecprivacy.org.

[30] Competition law, obviously, cannot be considered the sole source of inspiration for facilitating such cooperation. Cf. Recommendation 20, *infra*.

[31] By "European" competition law, we actually mean the one of the European Union. Enforcement cooperation therein is based on Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 04.01.2003, pp. 1–25. Its entry into force substantially modernized the enforcement of European competition law, marking a transition to a more decentralized one; therefore means of cooperation between the European Commission (Directorate-General for Competition) and national competition authorities (NCAs) needed to be established.

call for cooperation between relevant authorities. When it comes to cross-jurisdictional cases, both supervisory authorities in data privacy law and competition authorities have comparable needs: in both situations, in order to ensure efficiency and consistency, enforcement requires closer co-operation between competent authorities, e.g. assistance in evidence gathering and exchange of case-related information, including confidential or otherwise protected information. It is also likely that these two areas would face similar obstacles. Next, in both fields, certain basics for cooperation have been already developed: various formal and informal arrangements, of varying geographical reach, coexist (i.e. international, regional, and bilateral). In both fields, the convergence of legal frameworks facilitates cooperation, and *vice versa* (Kloza and Mościbroda 2014, 135). What differs these two is that enforcement cooperation in competition law has already achieved a relatively high level of efficiency while its counterpart in data privacy law still only aspires thereto.

Finally, it is *European* competition law that offers perhaps the most advanced, sophisticated and – what is sought in the data privacy area – *efficient* arrangement for enforcing its substantive provisions, which has proven useful over the past decade.[32] It is the European Competition Network (ECN) – established and governed by a directly binding regulation – that enforces substantive European competition law. The ECN is an example of cooperation between relevant authorities based on a clear legal basis, setting forth clear procedures, including those for an exchange of confidential information, and thus allowing closer cooperation. For that reason, it became a worldwide reference point for cooperation in competition and antitrust enforcement (Kloza and Mościbroda 2014, 132).

Inspired by these developments, Kloza and Mościbroda (2014) identified the core elements that make the functioning of ECN efficient with a view of improving analogous co-operation in data privacy law. It was revealed that cooperation should satisfy four legal requirements, namely: (1) a **firm legal basis**, which implies its **binding** nature,[33] and offers a structured and sufficiently detailed **set of rules**; (2) which define forms of cooperation, its conditions and **procedures**, including (3) provisions for the exchange of **confidential** or otherwise protected **information** (under appropriate conditions). Moreover, (4) such cooperation, in order to be effective, should have **geographical scope** as broad as possible.[34] It follows that from the formal point of view, each jurisdiction should have in place legal provisions allowing for enforcement cooperation between supervisory authorities and satisfying the four above-mentioned quality criteria. However, whether these legal provisions originate, for example, from an international treaty or are adopted unilaterally, is of secondary importance here. When the level of convergence of substantive laws on data so allows, it was argued that supervisory authorities could form a network or networks by means of an international agreement satisfying these four criteria.

A few of these criteria require some further explanation. It should be noted that a "firm legal basis" means that a legal instrument must be in place at national level and must satisfy certain criteria of both contents of the law and quality of law-making. From a broader perspective, this requirement can be translated into the principle of legality, which is rooted in Western liberal democracies. Among other international and European treaties, the principle of legality stems e.g. from the second paragraphs of Articles 8–11 of the European Convention on Human Rights (ECHR) and is recurrent in the case law of the European Court of Human Rights (ECtHR; Strasbourg Court). In particular, this case law refers to the interpretation of the expressions "in accordance with law"

[32] For an evaluation of a decade of functioning of the ECN, cf. European Commission, *Ten Years of Antitrust Enforcement under Regulation 1/2003: Achievements and Future Perspectives*, Brussels, 9 July 2014, COM(2014) 453.

[33] Thus far, in the field concerned, there exist two legal instruments that are based on a firm legal basis and are of a binding nature: (1) Convention 108 (cf. *supra note* 25) and the 1995 Data Protection Directive (cf. *supra note* 12).

[34] Emphasis ours.

or "prescribed by law", occurring in Articles 8–11 ECHR (Galetta and De Hert 2014). Although these deliberations are primarily applicable in cases of interference with a fundamental right, the conditions for the quality of law-making are equally applicable here. According to the established jurisprudence of the ECtHR, the phrase "in accordance with the law" [Article 8(2) ECHR] includes the following:

a. A norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen – if need be, with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail; however, experience shows that absolute precision is unattainable and the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague […].
b. The phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law; it thus implies that there must be a measure of protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by, *inter alia*, paragraph 1 of Article 8 […].
c. A law which confers a discretion is not in itself inconsistent with the requirement of foreseeability, provided that the scope of the discretion and the manner of its exercise are indicated with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference […].[35]

Furthermore, few readers would likely disagree that when it comes to enforcement, some level of compulsion must be maintained. Thus (at least) *enforcement* cooperation should be based on a legally binding instrument and engagement of supervisory authorities in such cooperation should be obligatory. Being lawyers, we tend to believe that if something were not compulsory, it would never happen. (Imagine the consequences of a criminal code being voluntary: you are brought to justice only if you want it.) (Kloza, van Dijk, and De Hert 2015). Currently, the non-binding nature of the majority of enforcement cooperation initiatives in data privacy law does not result in much concrete commitment and thus renders it inefficient.

We are convinced that these lessons from enforcement cooperation of relevant authorities in the field of European competition law are valid and relevant as they point out the desired direction of development of analogous cooperation in the area of data privacy law. We are further convinced that the majority of these lessons are applicable to any form of cooperation of the latter authorities, beyond mere enforcement. These recommendations can be applied to cooperation occurring at any level, from bilateral, to regional, to global.

Bearing this in mind, we will now develop a set of 23 recommendations in that direction, divided into legal (Section 4.1) and practical ones (Section 4.2), supplemented by a modest action plan (Section 4.3). We stress that these recommendations derive from our own work on the PHAEDRA project and our own experience therefrom. Thus, they represent, in a sense, our personal point of view as informed by our research. Each recommendation is substantiated with an explanatory text of a minimal length; we therefore invite the reader to consult the legacy documents of the PHAEDRA project for further details. For the sake of easiness of the policy-makers, we introduce each of our recommendation with a quotation from popular culture, in English, French, German, Latin and Polish.

[35] ECtHR, *Olsson v Sweden (No. 1)*, application No. 10465/83, judgment of 24 May 1988, § 61. The Court reached those findings in its previous cases *Sunday Times v the United Kingdom*, application No. 6538/74, judgment of 26 April 1979, § 47; *Silver and Others v the United Kingdom*, application No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, judgment of 25 March 1983, § 86; and *Malone v the United Kingdom*, application No. 8691/79, judgment of 2 August 1984, §§ 66–67.

4. Achieving efficiency of cooperation of supervisory authorities in the area of data privacy law

4.1 Legal recommendations to the attention of policy-makers

1. "Pourquoi faire simple quand on peut faire compliqué?" (Les Shadoks).[36] **The (legal) arrangement(s) and/or framework(s) for the cooperation of supervisory authorities in the area of data privacy law should be as clear, simple and easy-to-apply as possible. Unreasonable multiplication of the said arrangements and/or frameworks runs a risk of counter-productivity.**

The current legal framework on the basis of which supervisory authorities cooperate is a complex one. It required a large amount of research to identify the existing networks and to understand them and how they work. Our common sense suggests that if we spent quite some time to get to the bottom of this system, a lay citizen may hardly do so and will certainly encounter as many difficulties as we did. These difficulties become more concrete and tangible in case a lay citizen needs to contact one of those supervisory authorities as data subject to exercise one of her rights and/or to remedy a data privacy violation. Such situation gets even more complicated if such a violation is of a cross-border nature. Yet, the complexity of the existing cooperation arrangements and frameworks has a negative impact not only on data subjects but also on the other actors involved in this "business" namely data controllers or processors and supervisory authorities. Supervisory authorities, often supported by in-house legal experts, would probably somehow figure out how the system works. So will big businesses and organisations, but small or medium enterprises (SMEs) might need to resolve to legal help.

One can demonstrate a practical example to explain this complexity by referring again to EU data protection law. From the perspective of the data subject, data protection breaches can be remedied in three main yet non-exclusive ways. In particular, the data subject can seek remedy before the following entities (Galetta and De Hert 2015):

1. the data controller (or processor): access rights;
2. a supervisory authority;
3. national (or – in some cases – supranational) courts.

To add to this complication:

1. remedies may be sought by a data subject herself or by a proxy, e.g. an NGOs seeking remedy on her behalf;
2. supervisory authorities might act having heard a claim from an individual as well as *ex officio*;
3. in cross-border cases, procedural rules on how to remedy data privacy violations vary across jurisdictions;
4. finally, complaints and cases can be handled within various domains of law, ranging from administrative (if applicable) to civil and criminal law; the use of one does not usually preclude the use of any other.

In result, data subjects, data controllers and processors and supervisory authorities need to ask a series of questions, starting with the following ones: where should I go? A data subject would ask herself: which authority, in which jurisdiction, would deal with my case?; a data controller or processor: which authority or authorities would investigate and eventually fine me?; a supervisory authority: am I competent to deal with that case? Whom else shall I work with? Can I work with my colleagues in other jurisdictions? Should I work with them? Which available cooperation mechanism should I use? Etc. Etc.

[36] Ironic.

2. "Entia non sunt multiplicanda praeter necessitatem" (William of Ockham). **There *might be* no need to create a specific branch of law or specific legal constructions for the cooperation of supervisory authorities in data privacy law if existing legal tools, even if combined, can efficiently protect data privacy.**

Following the pervious recommendation, we simply mean that the (legal) arrangement(s) and/or framework(s) for the cooperation of supervisory authorities in data privacy law should not be made more complex than they are right now. For example, there is no need for two or more supervisory authorities to enter into a bilateral or multilateral agreement, concerning e.g. joint investigations, when their jurisdictions have already concluded such an agreement on a general level, applicable to more branches of law than data privacy law, e.g. a mutual legal assistance treaty (MLAT),[37] provided such a general arrangement satisfies minimum criteria of quality and efficiency.

Some further inspiration might come from EU private international law.[38] The Union, with a view to foster the development of the common market, of the area of freedom, justice and security as well as to broaden access to justice, has set rules for establishing jurisdiction, choosing the applicable law as well as recognizing and enforcing judgements (cf. e.g. van Calster 2013; Lookofsky and Hertz 2015). Although a detailed analysis thereof falls outside the scope of this chapter, a few instruments from this EU "toolbox" could be mentioned, e.g. Brussels I Regulation (new)[39] or European Enforcement Order for uncontested claims[40] – allowing for the automatic recognition and enforcement of judgements rendered in other Member States – or regulations for the service of documents,[41] taking of evidence[42] or for the European Certificate of Succession.[43] Using our example of joint investigations, some of these instruments might be of use for supervisory authorities in data privacy law (however, we acknowledge this will require further analysis) or might inform the development of cooperation arrangements and frameworks.

3. "I knew the stakes were high right from the start" (George Strait). **Since there are fundamental rights to privacy and personal data protection at stake, breaches of these rights, especially with cross-border implications, must be adequately addressed. Therefore, the framework(s) and arrangement(s) for the cooperation of supervisory authorities in the area of data privacy law must render the protection of these rights practical and effective.**

Since we talk about fundamental rights, their protection must be practical and effective. On the ground of the ECHR, the Strasbourg Court on numerous occasions, and most recently in *Nježić and* Štimac *v Croatia* (2015), observed that the "object and purpose of the Convention as an instrument for the protection of individual human beings require that [its provisions] be interpreted and applied so as to make its safeguards *practical* and *effective*".[44] These two core conditions are applicable to the whole "universe" of the protection of fundamental rights, including

[37] Cf. e.g. European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 20 April 1959, ETS 30; Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 07.11.2009, pp. 40–41.

[38] "Conflict of laws" in the Anglo-Saxon terminology.

[39] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012, pp. 1–32.

[40] Regulation (EC) No 805/2004 of the European Parliament and of the Council of 21 April 2004 creating a European Enforcement Order for uncontested claims, OJ L 143, 30.04.2004, pp. 15–39.

[41] Regulation (EC) No 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents), and repealing Council Regulation (EC) No 1348/2000, OJ L 324, 10.12.2007, pp. 79–120.

[42] Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters, OJ L 174, 27.06.2001, pp. 1–24.

[43] Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession, OJ L 201, 27.07.2012, pp. 107–134.

[44] ECtHR, *Nježić and Štimac v Croatia*, application No. no. 29823/13, judgment of 9 April 2015, § 61 (emphasis added).

data privacy, and thus apply equally to the legal framework for the cooperation of supervisory authorities in the area of data privacy law.

Moreover, Art 13 ECHR, ensuring the right to effective remedy, further safeguards such effectiveness. It stems from the Strasbourg Court case law that (Council of Europe 2013):[45]

> A remedy is only effective if it is available and sufficient. It must be sufficiently certain not only in theory but also in practice, and must be effective in practice as well as in law, having regard to the individual circumstances of the case. Its effectiveness does not, however, depend on the certainty of a favourable outcome for the applicant.
>
> Article 13 does not require any particular form of remedy, States having a margin of discretion in how to comply with their obligation, but the nature of the right at stake has implications for the type of remedy the State is required to provide. Even if a single remedy does not by itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided for under domestic law may do so. In assessing effectiveness, account must be taken not only of formal remedies available, but also of the general legal and political context in which they operate as well as the personal circumstances of the applicant.

4. "The user is always right" (popular adage)**. The closer to the individual the case is solved, the better. The arrangement(s) and/or framework(s) should be user-friendly.**

The position of a data subject is similar to that of a consumer: a data subject acts outside her "trade, business, craft or profession",[46] which – accordingly – places her in a weaker position on the market. This justifies certain protection measures. For example, Article 18 of the new Brussels I Regulation clearly states that:[47]

> 1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled.
> 2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled.

Therefore, authorities that are closer to the data subject and can interact with her should solve complaints and cases in data privacy matters.

5. "The more, the merrier" (popular adage). **In order to ensure "practical and effective" protection, supervisory authorities in the field of data privacy law should cooperate *also* with their counterparts in other areas of law (such as competition, consumer protection or criminal law) and judicial authorities, also in different jurisdictions, as long as their counterparts touch upon data privacy issues. They should also involve civil society organisations for this purpose, e.g. NGOs, unless inappropriate. They should not refuse cooperation with international or regional bodies (such as the Council of Europe) and networks of supervisory authorities. The legal system should explicitly permit for such cooperation. Various levels of cooperation – i.e. bilateral, multilateral, regional, supranational and international – should not mutually exclude each other but rather be complementary; this implies a careful design of interchanges between them.**

Data privacy is a cross-cutting subject and data subject's rights may deserve protection under different bodies of law such as consumer protection law, competition law, equality law, criminal law, etc. This reflects the need to establish and develop forms of cooperation among

---

[45] References to particular cases omitted. Cf. further: ECtHR, *Silver and Others v the United Kingdom*, application No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, judgment of 25 March 1983, § 113. ECtHR, *Leander v Sweden*, application No. 9248/81, judgment of 26 March 1987, § 77; (European Union Agency for Fundamental Rights 2014, 15–17).

[46] Directive 2011/83/EU of the European Parliament and of the Council of 25 OCTOBER 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, pp. 64–88; Article 2.

[47] *Supra note* 39.

different actors in these fields, also beyond borders of a single jurisdiction. These actors would include relevant supervisory authorities,[48] judicial authorities and administrative bodies as well as non-state actors, such as NGOs. Various networks and associations of these actors should be invited to cooperate as well.

All these actors may act at any level, i.e. bilateral, multilateral, regional, supranational or international. These levels should not exclude each other but rather should be complementary; this however requires clear delimitations between these. Conversely, in some cases, bilateral or multilateral cooperation, at a lower level than regional – e.g. closer to the individual, often applying much simpler and faster procedures – would be more efficient.

Therefore, the need for a broad involvement of different actors touching upon data privacy issues can be conceptualised on at least six levels: a supervisory authority in data protection law should (be able to) cooperate with:

1. supervisory authorities from other areas of law;
2. judicial authorities;
3. supervisory authorities from other jurisdictions:
   a. their counterparts,
   b. authorities from other areas of law,
   c. judicial authorities;
4. civil society organisations;
5. international or regional (public law) bodies;
6. networks of supervisory authorities, equally from the area of data privacy law or not.

6. "No matter where you go, I will find you" (Clannad). **Supervisory authorities in the field of data privacy law should be able to exercise, to a reasonable extent, extraterritorial jurisdiction.**

Nowadays data breaches have often cross-jurisdictional implications and – in order to ensure the practical and effective protection of the fundamental rights to privacy and personal data protection (as well as to an effective remedy) – these cross-border violations should be adequately addressed. Put simply, "law depends on it being taken seriously. Law depends on being enforced. Law depends on it being applied where it can and should be applied. Law cannot be confined to the nation state but must when appropriate have extraterritorial effect" (Blume 2014, 171). This, obviously, requires supervisory authorities to be able to exercise, to the necessary and reasonable extent, their powers in other jurisdictions.[49]

These authorities should have both subject-matter jurisdiction (i.e. the one over the type of a dispute concerned; *ratione materiae*) and personal jurisdiction (i.e. the one over the parties involved; *ratione personae*), but this ability cannot be unlimited. Svantesson argues that "extraterritorial jurisdictional claims are reasonable because if states do not extend their data protection to the conduct of foreign parties, they are not providing effective protection for their citizens" (2013).

However, technically speaking, states are generally reluctant to accept extraterritorial claims; this is a question of sovereignty, often understood in a Westphalian sense. As a possible solution, Svantesson (2015) proposes to distinguish a fourth form of jurisdiction – i.e. "investigative" one, in addition to the three classical ones: (1) prescriptive (legislative) – the power to enact legislation; (2) judicial (adjudicative) – the power to adjudicate a case; and (3) enforcement – "the power to enforce the law put in place, in the sense of arresting, prosecuting, and punishing an

[48] These relevant supervisory authorities most often would fall into the category of independent regulatory agencies (IRAs). Cf. (Schütz 2012).

[49] In classical terms, having extraterritorial jurisdiction means to be able to "exercise […] jurisdiction […] over activities occurring outside […] borders" (Senz and Charlesworth 2001), but – in the digital era – it shall rather refer to "the exercise of jurisdiction (that may well, but need not, be extraterritorial) [that] has any extraterritorial effect or implications" (Svantesson 2013).

individual under that law". He argues that:

> […] not least due to the increase in cross-border contacts stemming from the Internet, it is useful to also consider a fourth type of jurisdiction. Indeed, what we can call "investigative jurisdiction" protects a state's power to investigate a matter without exercising adjudicative jurisdiction, applying prescriptive jurisdiction, or enforcing actions against the subject of its investigation. It is particularly useful in the context of data privacy law and consumer protection – areas where complaints are often best pursued by bodies such as privacy commissioners/ombudsmen and consumer protection agencies (Svantesson 2015).

In other words, with investigative jurisdiction, the threshold of extraterritorial jurisdictional claims is lower and this makes it more acceptable for states. This is particularly important for the cooperation of supervisory authorities in data privacy law as a lot of their activities, if not a majority, would fall into that particular category.

7. "À la frontière, la liberté, une nouvelle vie va commencer" (Babylon Circus). **The arrangement(s) and/or framework(s) for cooperation of supervisory authorities in data privacy law should not permit data controllers and processors to escape liability for data privacy violations, in particular by establishing business in a particular place to be beyond the effective reach of the law of certain jurisdictions.**

Data controllers and processors, especially in the private sector, might wish to escape the possibility of being held liable for cross-jurisdictional data privacy violations by choosing the place of establishment in a jurisdiction where a supervisory authority does not cooperate with its foreign counterparts or where the level of data privacy protection is simply lower. They often view this scenario as an invitation to "shop" for a more favourable forum.[50] Such a situation is often detrimental for the data subject.

We see two problems here. First, if enforcement cooperation remains voluntary, some authorities might not wish to engage. In this situation, it is very likely that the enforcement of data privacy law would be stricter in those jurisdictions in which cooperation initiatives are in place and looser in those in which no such framework is in place.

Second, arrangement(s) and/or framework(s) for cooperation of supervisory authorities in data privacy law should be "minimally equal", that is, should foresee the same minimal consequences in case a violation of data privacy law occurs. This brings us to the question whether is it ever possible? *Rebus sic stantibus* this seems utopian, but a certain standard of protection of data privacy law at international and regional level should be guaranteed.

8. "Sharing is caring" (popular adage). **Whenever supervisory authorities start dealing with a cross-jurisdictional case, they should be obliged to notify so *ex officio* their counterparts concerned without undue delay. Subsequently, they should be able to exchange information relevant for the case, under appropriate safeguards.**

Put it simply, the ability to exchange case-related information is a prerequisite for any form of effective enforcement cooperation (Kloza and Mościbroda 2014, 136). The first step thereto is to be aware of a cross-border case being dealt with by all authorities concerned.

While the need for sharing information in enforcement cooperation in cross-border cases is hardly contestable, the problem of relevance of information might occur. In our view, it is not that all information related in one way or another to a case being dealt with would need to be exchanged among the authorities concerned. Rather, supervisory authorities should be able to

[50] Svantesson (2013, 73–75) rightly argues that the concept of forum shopping is mistakenly viewed as something „necessarily evil and undesirable". For example, a plaintiff's choice to sue in its home forum, e.g. in a consumer matter, is ordinarily not viewed as something abusive. We have already recommended proximity of a forum for the data subject in cross-border cases. The problem arises only when the concept of forum shopping is abused. In the data privacy law context, this would concern a number of data controllers and processors choosing the forum solely for their benefit.

determine themselves, on a case by basis, what constitutes relevant information before sharing them with their counterparts and provide justification therefor. If supervisory authorities have divergent opinions about relevance of information, they should be able to negotiate about that, to the extent permitted by law.[51] (E.g. perhaps under no condition authorities would share state secrets, but some other types of information, e.g. trade secrets, might be exchanged if higher safeguards are ensured. The latter might include for instance retention periods, limitations on use and further disclosure, and an obligation to ensure security and confidentiality.)

9. "The piano keys are black and white, but they sound like a million colours in your mind" (Katie Melua). **Cooperation among supervisory authorities should rely on comprehensive and harmonised legal "tools" and procedures to be used in cross-border cases. Extra-legal tools should supplement legal ones. To that end, some minimal "table of contents" for any arrangement(s) and/or framework(s) should be agreed in a first place.**
As of now, supervisory authorities have at their disposal a wide range of legal "tools" to be used in cross-border cases. A quick survey of these tools reveals, among others, joint investigations, sharing evidence, audits, class action litigation, privacy certification and seals. Yet, these tools are far from being harmonised, i.e. they might be at disposal of one of the authorities cooperating, but not of the other. Furthermore, one authority might not be able to accept some requests from its counterpart.
The harmonisation of these tools, supplemented by the approximation of relevant procedural norms, would strengthen enforcement in data privacy law. The biggest problem is to make a list of "items" this harmonisation should concern. We have found the 2010 APPA Cross-border Privacy Enforcement Arrangement (CPEA) to be one of the first instruments containing one of the most comprehensive suggestions, i.e. procedures for cross-border cooperation (§9), respecting and safeguarding confidentiality (§10), information sharing, including contact point designation and sharing experience (§11), and miscellaneous matters such as staff exchanges, costs, and disputes (§§12–15).[52] The non-binding Global Cross Border Enforcement Cooperation Arrangement,[53] adopted at 36th ICDPPC at Mauritius, can serve here as another example. It deals with issues ranging from reciprocity, confidentiality and respecting privacy and data protection principles, to coordination principles, resolving problems and allocation of costs, to the return of evidence and eligibility.
Similarly, the harmonisation of tools *prima facie* not concerned with enforcement can be of some use too, such as cross-border data breach notification, privacy and data protection impact assessments (PIA, DPIA), privacy enhancing technologies (PETs) and binding corporate rules (BCR). The same is true for "soft" measures, such as "naming and shaming" and guidance.

4.2 Practical recommendations to the attention of supervisory authorities themselves (predominantly)

10. "We know who you are, we know where you live" (Nick Cave and The Bad Seeds). **Supervisory authorities and their networks should get to know each other better and should know more both about themselves and about their work. Supervisory authorities should treat their counterparts as peers.**

[51] The problem here is not about data privacy laws as such, which are usually silent about any type of confidential or otherwise protected information (short of personal data themselves), but rather about national administrative laws, both substantive and procedural, that preclude sharing information in given situations.
[52] APEC, *Cooperation Arrangement Cross-border Privacy Enforcement*, 2010/SOM1/ECSG/DPS/013, 28 February 2010, http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013. pdf .
[53] Cf. http://www.privacyconference2014.org/media/16667/Enforcement-Cooperation-Agreement-adopted.pdf.

Although supervisory authorities already rather know each other – at the end of the day, the worldwide data privacy community is rather small – they should know *more* about themselves. Yet, as a prerequisite, they should not discriminate their counterparts and genuinely treat them as peers, i.e. there is no more "important" or "influential" authority in the community.[54]

To that end, first, they should know more about the enabling laws of their counterparts. This should include also soft law instruments (e.g. best practice) and those originating from international bodies, both formal and informal, e.g. ICDPPC, as well as practical documents (e.g. templates). We acknowledge the existence and benefits of several databases fed with such information (e.g. the International Privacy Law Library run by the World Legal Information Institute).[55] However, some of these databases are selective, not easily accessible or accurate or simply they are not yet widely known nor used. The key here is *comprehensiveness*: such a database should cover as many jurisdictions as possible, should be regularly updated and widely referred to. In addition, a manual or guidelines could append such a database, in particular summarising key knowledge about each supervisory authority. This will allow supervisory authorities to determine, in a first place, if they can engage in cooperation and in what type thereof, and, subsequently, roles, competences, powers, responsibilities and procedures used by their counterparts.

Second, although we assume all supervisory authorities have already exchanged their contact details (e.g. within WP29, CoE or GPEN), they should make sure they have designed contact points for each of the purposes of cooperation, e.g. for handling cases (enforcement), for public education and/or for mutual training. Such a contact list should not only include the top officials, but also key staff, especially those in charge of international relations and enforcement. It should be kept up-to-date.

Third, supervisory authorities should establish a common platform for the management of cross-border cases. (Or, whenever suitable, to use as many of existing platforms as possible or to make them interoperable.) This would be a closed, secure platform with layered access controls, where supervisory authorities would be notifying, without a delay, all cross-border cases they (wish to) deal with as well as other useful information, e.g. their enabling laws or lists of contact points. We are, however, aware that a single platform remains a wishful thinking and both policy-makers and supervisory authorities may resist this idea as: (1) not all jurisdictions would join, (2) not all jurisdictions would be sharing information of the same categories or relevance, and (3) not all jurisdictions would be satisfied with technicalities of such a platform, especially the level of security. (Cf. the idea to use GPEN platform running on the infrastructure of the US Federal Trade Commission (FTC), which is "not NSA-proof".)

Fourth, supervisory authorities should be constantly updated on what their counterparts do, what they are working on, what their main data privacy issues are, how the most controversial topics in this area have been solved by their counterparts and/or in other jurisdictions.

11. "Better three hours too soon than a minute too late" (William Shakespeare). **Legal framework should permit supervisory authorities to act *speedily* upon any cross-border data privacy law breach, including the indication of interim measures, also *ex officio*.**

In our digital era, a timely reaction is of utmost importance. It follows that any action undertaken too late, *post factum*, does not necessarily stop nor remedy a violation. (Experience gathered that way might prove beneficial for instructive purposes.) Yet, the likelihood of supervisory authorities to act speedily does not only depend on their willingness, determination, experience and expertise, but predominantly on legal arrangements, especially on the availability of devoted cooperation tools. In particular, whenever a cross-jurisdictional

[54] Yet we notice that this principle of equality amongst supervisory authorities is a bit nuanced, as e.g. for certain types of cooperation, e.g. enforcement, their enabling legislation might impose some limits, concerning e.g. independence. Yet this recommendation is more for the development of a general attitude towards cooperation.

[55] Cf. http://www.worldlii.org/int/special/privacy.

violation of data privacy laws is likely to produce an imminent risk of irreparable harm, supervisory authorities should be able to indicate interim measures, not only on the request of a data subject.

12. "An ounce of prevention is worth a pound of cure" (Benjamin Franklin). **Supervisory authorities should take the lead in preventing data privacy violations from occurring, including cross-border ones, rather than focusing solely on *ex post* investigation and prosecution. Therefore, cooperation should be extended to all of their powers and duties, and should not regard only enforcement.**

This recommendation is meant for policy-makers and supervisory authorities to pay equal attention to the forms of cooperation other than enforcement, such as public education and internal trainings as well as contribution to policy-making and standard setting, with a view to more efficiently protect data privacy. Initiatives such as the European Data Protection Day,[56] the Privacy Awareness Week[57] or the ARCADES project[58] have proven useful. Likewise, the strengthening of preventative tools such as privacy and data protection impact assessments may help reach this purpose (cf. Recommendation 9).

13. "All we ever want is more, a lot more than we had before" (Shania Twain). **Supervisory authorities need appropriate *financial*, *human* and *technical* resources to carry out their duties and exercise their powers in the context of cooperation. In addition to the need to react fast to an alleged violation (cf. Recommendation 11), the legal framework should ensure them reasonably enough *time* to investigate cross-border data privacy law breaches.**

It is of paramount importance for supervisory authorities to be endowed with sufficient financial, human and technical resources to efficiently deal with cross-border cases and other forms of cooperation. Currently, the problem of resources represents one of the greatest obstacles limiting their activity (European Union Agency for Fundamental Rights 2014, 37–46). For example, as a means to remedy that, Article 47(5) GDPR establishes that:

> [e]ach Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the European Data Protection Board.

Although this provision should be welcomed, it is unclear how EU Member States would be able to ensure "adequate" resource endowments. Similarly, it is not yet clear which criterion will be used by Member States to fix that target.

14. "A man with a conviction is a hard man to change" (Leon Festinger). **Supervisory authorities must be genuinely convinced that engaging in cross-border cooperation is beneficial for the mission they realize.**

Motivation is key in any cooperation initiative and represents its baseline. Supervisory authorities do not usually engage themselves in cooperation unless they share common interests and concerns (Barnard-Wills and Wright 2014). Although this is more than reasonable, we find that cooperation is needed in cross-border cases, regardless of whether or not a supervisory authority expressed prior interest in a certain issue or topic. Moreover, if supervisory authorities cooperate efficiently and

[56] Data Protection Day, celebrated each year on 28 January, commemorates the anniversary of the opening for signature of the Council of Europe's Convention 108 for the Protection of individuals with regard to automatic processing of personal data. Cf. http://www.coe.int/dataprotection.

[57] Privacy Awareness Week (PAW) is an initiative of the Asia Pacific Privacy Authorities forum (APPA) held every year, across the Asia Pacific region by APPA members, to promote awareness of privacy issues and the importance of the protection of personal information. Cf. http://www.privacyawarenessweek.org.

[58] Cf. "Introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union"; http://arcades-project.eu.

effectively, there is no better result or outcome each of them would have reached alone. Yet, it has to be recognised that cooperation requires some prerequisites such as trust among peers, commitment, communication, regularity of interaction and inclusiveness, which cooperation itself cannot guarantee.

15. "Deine Zauber binden wieder" (Friedrich Schiller). **The worldwide cooperation of supervisory authorities in the area of data privacy needs encouragement from the authorities themselves as well as from policy-makers, in particular from international and supranational ones, such as the OECD, APPA, Council of Europe or the European Union. These bodies should set (a) standard(s) for efficient cooperation, perhaps one(s) to be formalized.**
In the first place, cooperation of supervisory authorities in the area of data privacy law needs support from those who shape their enabling legislation, and secondly – as it is a cross-jurisdictional matter – their cooperation needs such high-level support predominantly at supranational and international levels. We acknowledge that both governmental and non-governmental bodies such as European Union, Council of Europe, Organization for Economic Cooperation and Development (OECD) or Asia-Pacific Privacy Authorities (APPA) already support this cooperation. However, we believe further efforts are indispensable. To that end, for example, standardisation bodies, such as International Organization for Standardization (ISO) or UN International Law Commission, should contribute thereto by developing (a) standard(s) or model law(s) for cooperation. (For the contents thereof, cf. Recommendation 9). Further hopes are vested in international NGOs and advocacy groups as well as in the recently appointed UN Special Rapporteur to the Right to Privacy in the Digital Age.[59]

16. "Training is everything. The peach was once a bitter almond; cauliflower is nothing but cabbage with a college education" (Mark Twain). **Supervisory authorities should continue to enhance their efforts in mutual exchange of know-how by means of study visits, seminars and/or staff exchange.**
Any effort to exchange know-how among supervisory authorities should be welcomed and should be encouraged as means towards the efficiency of cooperation. The mutual exchange of expertise and competences should be promoted at all levels and be targeted to any person working within supervisory authorities, from senior managers to secretaries. Fellowship programmes, for instance, are fit for this purpose. For example, the FTC has established the International Fellows Program, which – since 2007 – has hosted 52 staff members from sister agencies around the world.[60]
However, it should be recognised that not all supervisory authorities have enough resources to finance these programs and/or are lucky enough to have access to them. In this latter case we find that seconded national experts programs, which are quite common in the public sector, represent the most appropriate solution. These programs would allow for the mutual exchange of expertise, but without too much burden for the supervisory authority hosting the "external" expert.

17. "Et je voudrais pouvoir un jour enfin te le dire, te l'écrire, dans la langue de Shakespeare. (...) Je ferais mieux d'aller choisir mon vocabulaire pour te plaire dans la langue de Molière" (Charles Aznavour). **Supervisory authorities need to clearly understand themselves, their work and their "clients", i.e. data subjects and data controllers or processors. Despite English being almost the *lingua franca*, they need to establish procedures for interpretation and translation of meetings and information shared.**

[59] United Nations, Human Rights Council, The right to privacy in the digital age, Resolution 28/16, 1 April 2015, A/HRC/RES/28/16; http://www.ohchr.org/EN/HRBodies/SP/Pages/HRC29.aspx.
[60] Cf. https://www.ftc.gov/internationalfellows.

Cross-border cooperation of any type will engage supervisory authorities using different languages. In order to ensure effective and smooth communication, procedures for translation and interpretation must be established. A few possible scenarios:

1. in their communication, authorities might select a single language or choose "bridging" languages, a solution somehow known from patent law, in which the core of a patent document (i.e. patent claims) should be published in English, French and German;[61]
2. supervisory authorities, for the purposes of sharing information, while determining its relevance, might translate it to the recipient's language;
3. a data subject might be offered to address her complaint concerning a cross-border violation in her own language or in English (or any other "bridging" language). The advantage for the data subject to opt for English is that most probably in this latter scenario her case will be dealt faster. Yet, supervisory authorities themselves have to make sure that the right to an effective remedy in data privacy law is guaranteed to everyone, regardless of obstacles posed by translation (cf. Recommendation 3);
4. in case of the foreseen EDPB, the Directorate-General for Translation of the European Commission (DG-T) should ensure official translation and interpretation of the case-related material and communication. At the stages where official translation and interpretation is not yet required, supervisory authorities might rely on the language skills of their personnel.

Inevitably connected with translation and interpretation is the question of covering their costs, which should not refrain supervisory authorities from cooperating among each other.

18. "We'll go Dutch, shall we?" (popular adage). **Supervisory authorities should reach an agreement on the way of covering the costs of cooperation. The establishment of a system for the mutualisation of costs should not be excluded.**

Cooperation of any type involves many activities and they come at a price. A clear and fair solution is necessary to establish who should cover what costs. As one of the solutions, each authority could cover their own costs of cooperation or there could be a common budget among supervisory authorities from which cross-jurisdictional activities would be funded. This latter scenario takes into account the fact that not all supervisory authorities dispose of enough resources to get involved in cooperation activities. Hence, systems of mutualisation of costs among supervisory authorities should be equally foreseen.

4.3 An action plan for the development of efficient cooperation

19. "All we have to decide is what to do with the time that is given to us" (J.R.R. Tolkien). **An agenda for the development of the framework for the cooperation of supervisory authorities in the area of data privacy should be developed, prioritizing the most urgent, concrete and pertinent issues to be addressed. Efficient cooperation in data privacy law should be a stepping stone rather than a stumbling block.**

Much ink has been already spilled over about the idea of, the need for, the benefits of, the barriers against and other problems related to coopertion between supervisory authorities. These remain valid, but now there is a need to discuss more concrete, down-to-earth issues.

This challenging goal should be pursued by prioritizing the most urgent issues in data privacy law and by developing cooperation with a step-by-step approach. As it is argued in international economics, the development of efficient cooperation may be seen as a stumbling block

[61] "The official languages of the European Patent Office shall be English, French and German. […] A European patent application shall be filed in one of the official languages or, if filed in any other language, translated into one of the official languages in accordance with the Implementing Regulations"; Article 14(1)-(2) of the Convention on the Grant of European Patents (Munich, 5 OCTOBER 1973), http://www.epo.org/law-practice/legal-texts/epc.html.

or a stepping stone (Bhagwati 1991; Lamy 2002). Recalling these two metaphors, we definitely see cooperation among supervisory authorities as a stepping stone (rather than a stumbling block), that is as a process, which develops gradually, resulting in an ever increasing degree of cooperation.

20. "Everybody's gotta learn sometime" (The Korgis). **In designing the framework for the cooperation of supervisory authorities in the area of data privacy, lessons should be learnt from cooperation in other areas of law, such as competition law, customs, consumer protection, securities, taxation, and criminal law, among others.**
Research conducted earlier, in particular the comparison with enforcement cooperation in European competition law (cf. Section 3) showed that cooperation in data privacy law might be improved also by looking at forms of cooperation among supervisory authorities that exist in other areas of law. It was very instructive to analyse experiences of cooperation developed in competition law. Yet, this kind of comparative "exercise" should be deepened and extended also to other legal fields.

21. "Nie od razu Kraków zbudowano" (popular adage). **Stakeholders should bear in mind that the development of an efficient framework for cooperation is a time-consuming process. Also, it will take even more time to test and validate such a framework in practice. Hence, some controversial elements of these frameworks could be possibly accompanied by a revision clause**.
As stressed earlier, in spite of the increasing proliferation of cooperation networks and mechanisms, cooperation in data privacy law is still in its infancy. Moreover, once a cooperation framework is established, it needs somehow to be tested by the concerned supervisory authorities. In order for cooperation to be efficient, these frameworks should allow for a certain level of flexibility, so that to avoid any problem that may arise in the implementation phase. It would be useful, for instance, to foresee a revision clause in the EU "one-stop-shop" mechanism, which thus far has raised a lot of controversies.

22. "The first thing we do, let's kill all the lawyers" (William Shakespeare). **Means of regulation other than law could be taken into consideration while developing a framework for the cooperation of supervisory authorities in the area of data privacy.**
There is a wide repertoire of tools and techniques that are used in regulating social behaviour (Morgan and Yeung 2007, 79). Based upon the "modality" of control primarily in operation,[62] Lessig's influential "pathetic dot theory" distinguishes four constrains that regulate human behaviour: law, market, social norms and architecture (code) (Lessig 2006, 121–125). Acknowledging that no scheme of classification is watertight, Morgan and Yeung more or less agree with Lessig, but they differentiate five methods of regulation: command and control, competition and economic instruments, consensus, communication and techno-regulation (code) (2007, 79–149). Each of these "modalities" can influence each other, each of them produces the best effects in different contexts, and each of them has its own advantages and disadvantages.
Similarly to the observation of Kloza, van Dijk, and De Hert (2015) on addressing smart grids challenges in the EU, it seems that possibilities other than law to address the issue of cooperation among supervisory authorities have not been explored nor used. Therefore, attention could be given to the choice and combination of other means that could regulate behaviour. This will have to be done by careful consideration of the constraints of the different practices in which these "regulators" are brought about.

[62] This does not preclude the fact that frequently these "modalities" are *introduced* by legal means.

23. "Et si tu crois que c'est fini, jamais!" (Céline Dion and Garou). **The data protection reform in the EU will not stop in 2015 and there is a tight agenda to do.**
The passing of the GDPR, if ever occurring, would not be the end of the data protection reform in the EU. Yet, as far as cooperation among supervisory authorities is concerned, we see the need for *at least* two further actions:

1. While the cooperation among EU supervisory authorities is extensively addressed in the proposed GDPR, this is not the case for cooperation with their extra-EU counterparts (Article 45 GDPR): the proposal does not provide a detailed picture as to how cooperation at international level should take place. The European Commission is tasked with the development of specific cooperation arrangements and frameworks with "third countries or international organisations". Perhaps such phrasing was a conscious choice as extra-EU cooperation cannot be of a uniform nature and specific arrangements and frameworks must be developed for each jurisdiction or for a group thereof.
2. Regulation 45/2001[63] would need to be replaced in order to live up to the adopted GDPR, putting the European Data Protection Supervisor (EDPS) back into the new data protection focus.

5. Conclusion: drawing a line between binding and non-binding types of cooperation in data privacy law

In this chapter we have provided an admittedly patchy picture of how cooperation among supervisory authorities in data privacy law could be developed with a view to increase efficiency or, at least, work in practice. Though, the proposed recommendations do not represent "the" solution, they do constitute a first attempt to improve the existing cooperation frameworks and arrangements by providing some modest suggestions, which are not necessarily exhaustive.

In this chapter, we have proposed and explained twenty-three solutions to the problem of inefficiency of the *status quo* of such cooperation. As a conclusion, we would like to attempt to draw a line between binding and non-binding types of cooperation. Why? Both policy-makers and supervisory authorities will need to decide, step-by-step, on both legal and extra-legal tools to be used and on compulsoriness of their choices, should they go for any of the proposed solutions.
We argue that such cooperation should be, to a large extent, voluntary, yet, once involved, binding for the supervisory authorities concerned. In other words, cooperation should become binding when supervisory authorities voluntarily decide to formally engage therein. However, when it comes to the *enforcement* of data privacy laws *sensu stricto*, there appears to be no other option than making such cooperation obligatory.

Recalling the enforcement cooperation spectrum elaborated by Baggaley (2014), we hold that the earlier stages or degrees of cooperation, i.e. those from sharing non-confidential information to coordinated compliance activities, should rather be non-binding. Some level of flexibility should be allowed whenever relevant information is being shared and such information is confidential. Here supervisory authorities may (voluntarily) engage themselves in binding frameworks and arrangements and their decision to do so shall be driven by the "gravity" of cases. However, binding arrangements are indispensable the case of formal enforcement cooperation. Hence, in this perspective Baggaley's enforcement cooperation spectrum illustrated earlier at Fig. 1 could be now revised as shown in Fig. 3.

[63] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, pp. 1–22.

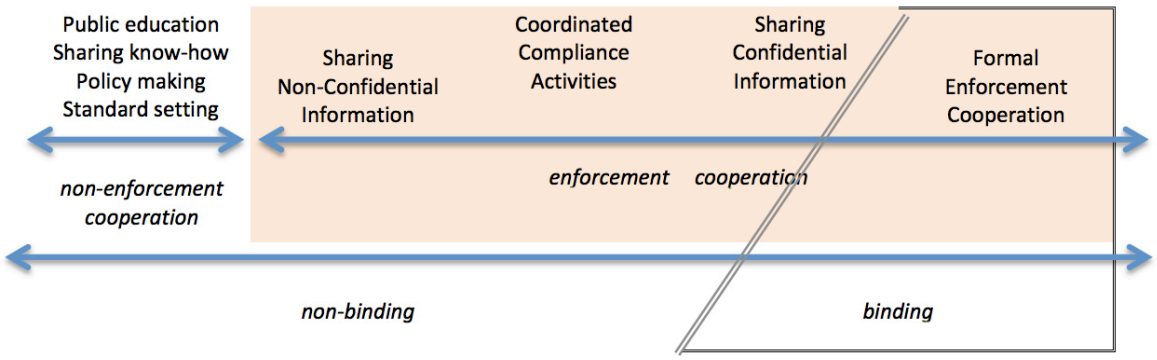

Figure 3. The (revised) cooperation spectrum

Thus, the challenging goal of efficiency should not be reached by using "hard" forms of cooperation only. Instead, we would recommend that it is not only necessary to see black and white aspects of the picture, but also those many shades of grey in-between. Efficiency should be sought by letting supervisory authorities appreciate those many nuances and the benefits of cooperation itself.

6. References

6.1 Literature

Baggaley, C. 2014. "International Enforcement Cooperation: The OPC Perspective". In *Enforcing Privacy: Lessons from Current Implementations and Perspectives for Future. Final Conference of the PHAEDRA Project [Improving Practical and Helpful cooperAtion bEtween Data pRotection Authorities]. Kraków, 12 December 2014*. http://www.phaedra-project.eu/wp-content/uploads/Carman-Baggaley.pdf.

Barnard-Wills, D. and D. Wright. 2014. *Co-Ordination and Co-Operation between Data Protection Authorities*. Deliverable D1 of the PHAEDRA project [Improving Practical and Helpful cooperAtion bEtween Data pRotection Authorities]. London. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf.

Bennett, C. and Ch. D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. MIT Press.

Bhagwati, J N. 1991. *The World Trading System at Risk*. Harry Johnson Memorial Lecture. Princeton University Press.

Blume, P. 2014. "Dan Jerker B. Svantesson, Extraterritoriality in Data Privacy Law [Review]". *International Data Privacy Law* 4 (2): 171–73. doi:10.1093/idpl/ipu003.

Bygrave, L. A. 2014. *Data Privacy Law: An International Perspective*. OUP Oxford.

Council of Europe. 2013. *Guide to Good Practice in Respect of Domestic Remedies*. Strasbourg. http://www.echr.coe.int/Documents/Pub_coe_domestics_remedies_ENG.pdf.

European Union Agency for Fundamental Rights. 2010. *Data Protection in the European Union: The Role of National Data Protection Authorities Strengthening the Fundamental Rights Architecture in the EU II*. Luxembourg: Publication Office of the European Union. doi:10.2811/47216.

———. 2014. *Access to Data Protection Remedies in EU Member States*. Luxembourg: Publications Office of the European Union. doi:10.2811/51206.

Galetta, A. and P. De Hert. 2014. "Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance".

Utrecht Law Review 10 (1): 55–75. http://www.utrechtlawreview.org/index.php/ulr/article/view/257.

———. 2015. "The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-Oriented Remedial System?" *Review of European Administrative Law (REALaw), 8 (1): 123–149*.

Kloza, D. and A. Mościbroda. 2014. "Making the Case for Enhanced Enforcement Cooperation between Data Protection Authorities: Insights from Competition Law". *International Data Privacy Law* 4 (2): 120–38. doi:10.1093/idpl/ipu010.

Kloza, D., A. Mościbroda, and G. Boulet. 2013. "Improving Co-Operation Between Data Protection Authorities: First Lessons from Competition Law". *Jusletter IT. Die Zeitschrift Für IT Und Recht*. http://jusletter-it.weblaw.ch/issues/2013/20-Februar-2013/2128.html.

Kloza, D., N. van Dijk, and P. De Hert. 2015. "Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies." In *Smart Grid Security. Innovative Solutions for a Modernized Grid*, edited by Florian Skopik, 11–46. Elsevier Ltd.

Kuner, C., F. H. Cate, C. Millard, and D. J. B. Svantesson. 2014. "Taking Stock after Four Years". *International Data Privacy Law* 4 (2): 87–88. doi:10.1093/idpl/ipu009.

Lamy, P. 2002. "Stepping Stones or Stumbling Blocks? The EU's Approach Towards the Problem of Multilateralism vs Regionalism in Trade Policy". *World Economy* 25 (10). Blackwell Publishers Ltd: 1399–1413. doi:10.1111/1467-9701.00498.

Lessig, L. 2006. *Code Version 2.0*. http://www.codev2.cc/download+remix/Lessig-Codev2.pdf.

Lookofsky, J. M. and K. Hertz. 2015. *EU-PIL: European Union Private International Law in Contract and Tort*. Huntington, NY: JuristNet, LLC.

Morgan, B. and K. Yeung. 2007. *An Introduction to Law and Regulation: Text and Materials*. Law in Context. Cambridge University Press.

Raab, Ch. D. 2010. "Information Privacy: Networks of Regulation at the Subglobal Level". *Global Policy* 1 (3): 291–302. doi:10.1111/j.1758-5899.2010.00030.x.

———. 2011. "Networks for Regulation: Privacy Commissioners in a Changing World". *Journal of Comparative Policy Analysis: Research and Practice* 13 (2): 195–213. doi:10.1080/13876988.2011.555999.

Schütz, P. 2012. "The Set Up of Data Protection Authorities as a New Regulatory Approach". In *European Data Protection: In Good Health?*, edited by S. Gutwirth, R. Leenes, P. De Hert, and Y. Poullet, 125–42. Springer Netherlands. doi:10.1007/978-94-007-2903-2_7.

Senz, D. and H. Charlesworth. 2001. "Building Blocks: Australia's Response to Foreign Extraterritorial Legislation". *Melbourne Journal of International Law* 2 (1): 69–121. http://search.informit.com.au/documentSummary;dn=317555450176533;res=IELHSS.

Stewart, B. 2013. "Cooperation beyond DPAs". In *Improving Cooperation and Coordination between DPAs. PHAEDRA 1st Workshop, Warsaw*. 24 September 2013. http://www.phaedra-project.eu/wp-content/uploads/Blair-Stewart_-PHAEDRA.pdf

Svantesson, D. J. B. 2013. *Extraterritoriality in Data Privacy Law*. Copenhagen: Ex Tuto Publishing.

———. 2015. "Will Data Privacy Change the Law?" *OUPblog*. http://blog.oup.com/2015/05/investigative-jurisdiction-law/.

Toonders, J. 2014. "Data Is the New Oil of the Digital Economy". *Wired*.

http://www.wired.com/2014/07/data-new-oil-digital-economy/.

Van Calster, G. 2013. *European Private International Law*. Oxford: Hart Publishing.

Wright, D. and P. De Hert. 2015. "Introduction to Enforcing Privacy". In *Enforcing Privacy*, edited by D. Wright and P. De Hert. Springer *(forthcomming)*.

6.2 Translations and sources of quotations in the text

Every effort has been made to trace and identify copyright holders. The publisher apologizes for any errors or omissions in the below list and would be grateful if notified of any corrections that should be incorporated in future reprints or editions of this book.

1. "Why make things simple when they can be complicated?" [translation ours]; from "Les Shadoks", directed by René Borg, scenario René Borg; ORTF 1968–1974.
2. "Entities should not be multiplied beyond necessity" [translation ours]; attributed to William of Ockham (ca. 1285–1349), though not found in his writings.
3. From "The Cowboy Rides Away" by George Strait, written by Kelly/Throckmorton, 1985.
6. From "I Will Find You" by Clannad, written by Brennan/Ciaran Marion, 1994.
7. "At the frontier – liberty, a new life will start" [translation ours]; from "Marions-nous au soleil" by Babylon Circus feat. Karina Zeviani, written by Baruchel, Faupin, Dirat, Nectoux / Faupin, Chaccour, Dirat, 2009.
9. From "Spider's Web" by Katie Melua, written by Melua/Melua, 2005.
10. From "We No Who U R" by Nick Cave and The Bad Seeds, written by Cave/Cave, 2013.
11. William Shakespeare, "The Merry Wives of Windsor", Act 2, Scene 2.
12. Benjamin Franklin writing anonymously as an "old citizen" in February 4, 1735 edition of the "Pennsylvania Gazette". Cf. Kiel, Daniel. 2011. "An Ounce of Prevention Is Worth a Pound of Cure: Reframing the Debate about Law School Affermative Action." Denver University Law Review 4 (88): 791–806, note 3.
13. From "Ka-Ching" by Shania Twain, written by Lange/Twain, 2002.
14. Leon Festinger, "A theory of cognitive dissonance", Stanford University Press, 1962.
15. "Your magic reunites" [translation ours]; from Friedrich Schiller, "An die Freude", 1785.
16. Mark Twain, "The Tragedy of Pudd'nhead Wilson", 1894.
17. "And I would like at last to be able to tell you that, to write you that, in the language of Shakespeare's tongue. […] I would better pick my vocabulary to please you in the language of Molière" [translation ours]; from "For Me... Formidable" by Charles Aznavour, 1963.
19. J.R.R. Tolkien, "The Fellowship of the Ring", 1954.
20. From "Everybody's Got to Learn Sometime" by The Korgis, written by Warren, 1980.
21. The same proverb in English: "Rome wasn't built in a day".
22. William Shakespeare, "Henry VI", Part 2, Act 4.
23. "If you think it's over, never!" [translation ours]; from "Sous le vent" by Céline Dion and Garou, written by Veneruso/Battagli, 2000.

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: paul.de.hert@vub.ac.be

N°1 **"The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area"** by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 **"The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection"** by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 **"Towards efficient cooperation between supervisory authorities in the area of data privacy law"** by Dariusz Kloza, Antonella Galetta (24 pages)