Data protection authority perspectives on the impact of data protection reform on cooperation in the EU

David Barnard-Wills, Cristina Pauner Chulvi, Paul de Hert

Abstract

This article presents the findings of interviews with representatives from the majority of EU data protection authorities in the context of the ongoing data protection reform process. It identifies commonalities between the authorities to the extent it is possible to speak about a EU DPA perspective, but also identifies areas of tension and disagreement as well as future intentions. The focus of the article is upon the impact of the data protection reform process on the way that these independent bodies, located in EU Member States will increasingly have to cooperate at an EU-level. Capturing these perspectives at this moment in the reform process provides insight into the process from a group of concerned stakeholders, but also insight into how these stakeholders are (re)positioning themselves, planning, and anticipating the impacts of the reform.

Keywords

Data protection, privacy, General Data Protection Regulation, reform, enforcement, international cooperation, European Union, Data protection authorities.

1. Introduction

European Union Data Protection Authorities (DPAs) are independent authorities (with their own powers and responsibilities, and organisationally separate from Member State ministries[1]) with a supervisory role in relation to data protection. Within the EU, they primarily draw their authority from the national implementations of Directive 95/46/EC - the Data Protection Directive. Globally, DPAs (also known as privacy commissioners, data privacy agencies and privacy enforcement authorities[2]) play multiple roles, such as ombudsmen, auditors, consultants, educators, policy advisors and negotiators as well as conducting enforcement actions.[3] The data protection legal regime in the EU is currently undergoing a reform process: The General Data Protection Regulation (GDPR) and the associated Police and Criminal Justice Data Protection Directive are intended to reform and update the 1995 EU Data Protection Directive and replace the 2008 Framework decision.[4] At

[1] Thatcher, Mark, "Regulation after delegation: Independent Regulatory Agencies in Europe", *Journal of European Public Policy*, Vol. 9, No.6, 2002, p. 956

[2] OECD, Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, Paris, 2007, http://www.oecd.org/internet/interneteconomy/38770483.pdf

[3] Bennett, Colin & Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge MA & London, 2003, pp.109-114

[4] de Hert, Paul, Vagelis Papakonstantinou, David Wright & Serge Gutwirth, "The proposed Regulation and the construction of a principles-driven system for individual data protection", *Innovation: The European Journal of Social Science Research*, Vol.26, No.1-2, 2013, pp.133-144; Kuner, Christopher, "The European Commission's Proposed Data Protection Regulation: a Copernican revolution in European Data Protection Law, *Privacy and Security Law Report*, The Bureau of National Affairs, 02/06/2012; Costa, Luiz & Yves Poullet, *Privacy and the Regulation of 2012*, *Computer Law and Security Review*, 28, 2012, pp.254-262.

the time of writing, the Commission, the European Parliament and the Council have adopted positions on the Regulation and have completed the trialogue negotiation process producing a compromise text that will be formalised over the coming months. The resulting adopted text is likely to have significant impacts for EU DPAs. These impacts are likely to be particularly significant on the way in which EU DPAs cooperate with each other in a number of registers. Networking and group formation amongst DPAs have been ongoing for some time[5] and Europe is seen as a particular concentration of such activity, given the role of the Article 29 data protection working party as a point of discussion and coordination, and the coming together of EU DPAs in events such as the Spring Conference, and the Berlin Group. Collaboration outside of enforcement provides opportunities for DPAs to increase their regulatory capacity and effectiveness in relation to globalised threats to privacy.[6] However, the GDPR will place increased requirements for collaboration upon EU DPAs.

Given their ambiguous position of organisations that are likely to be deeply affected by the GDPR; responsible for enacting elements of it; and likely to have at least some of their manner of working restructured by it, but at the same time having limited official input into its final form, the perspective of EU DPAs on the reform process is particularly relevant. Capturing these perspectives at this moment in the reform process provides insight into the process from a group of concerned stakeholders, but also insight into how these stakeholders are (re-)positioning themselves, planning, and anticipating the impacts of the reform. This article is therefore intended to contribute to the literature on the international relations of data protection authorities. Cooperation between DPAS has become the subject of a relatively small number of previous articles[7], many of which engage with the extent to which there is an emerging field of interaction between these actors engaged in cross-border interaction, and the extent to which the development of multi-level governance can be identified. This article expands this picture with the perspective of EU DPAs themselves. Their perceptions, anticipated challenges, problematisations and how they construct past experiences will impact upon the development in practice of EU governmentality (regimes of shared practice operating in spaces beyond, around and between states[8]) around privacy and data protection post-GDPR.

---

[5] Barnard-Wills, David & David Wright, *Co-ordination and co-operation between Data Protection Authorities*, PHAEDRA Project Workstream 1 report, April 2014 revised June 2014. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf; Wright, David & Kush Wadhwa, "Cooperation and Coordination viewed by supervisory authorities themselves: Result of the PHAEDRA surveys" in Paul De Hert, Dariusz Kloza & Pawel Makowski (eds.) *Enforcing Privacy: Lessons from current implementations and perspectives for the future*, Warsaw, Wydawnictwo Sejmowe, 2015. http://www.phaedra-project.eu/wp-content/uploads/phaedra1_enforcing_privacy_final.pdf

[6] Raab, Charles, "Information Privacy: Networks of Regulation at the Subglobal level", *Global Policy*, Vol.1, No. 3, October 2010, pp.291-302.

[7] Ibid ; Bygrave, Lee A., *Data Protection Law. Approaching Its Rationale, Logic and Limit*, Kluwer Law International, The Hague / London / New York, 2002; Raab, Charles & Paul de Hert, "Privacy actors, performances, and the future of privacy protection in Serge Gutwirth, Yves Poullet, Paul de Hert & C. de Terwange & S. Nouwt (Eds), *Re-inventing data protection?*, Dordrecht, Springer, 2009; Newman, A., *Protectors of Privacy: Regulating Personal Data in the Global Economy*, Ithaca, NY, Cornell University Press, 2008.

[8] Dean, Mitchell, *Governmentality: Power and Rule in Modern Society, 2nd Edition*, London, Sage, 2010, p. 229

The paper first provides an account of the interview methods deployed in this study, before examining DPA perspectives on the GDPR and its impacts upon cooperation, in particular, the consistency mechanism, the "one-stop-shop" principles, the European Data Protection Board, the trialogue process, and information sharing. It then examines DPA perspectives on cooperation frameworks more broadly, including the possibilities of structured systems for information exchange, sharing best practice, requests for assistance, the role of the European Commission, complaint handling, alerting tools and budgets for cross border investigations.

The paper finds that DPAs anticipate a significant impact from the GDPR, particularly for their inter-EU cooperation. The GDPR is seen as likely to increase the need for cooperation and to structure the form that this cooperation will take. As the reform process is still ongoing there is ambiguity about the final text, but even beyond that DPAs anticipate they will need to conduct further work on the practical details of cooperation. DPAs are concerned to build upon positive existing cooperation and communication methods. Key challenges for DPAs include maintaining legitimacy, freedom of action and ability to determine their own strategies and methods, and ability to take what they see as appropriate measures, whilst maintaining coordination and consistency with their peers. Open debates include the extent to which the GDPR will effectively harmonise data protection across Europe, and which elements of strategic independence and national context will remain for DPAs. Further, the extent to which structured processes and common approaches are possible or desirable is still an open question, with different DPAs holding different positions. Language differences remain a key topic of discussion in these interviews, potentially exacerbated by the type and volume of communication required under the reforms.

2. Methods

A series of semi-structured interviews were conducted with senior representatives of European Data protection authorities between April and May 2015. The authors interviewed 27 representatives, covering nearly all Member State national DPAs, one German state DPA (Landesbeauftragter für Datenschutz) representative[9] and the European Data Protection Assistant Supervisor. These interviews lasted between 30 to 75 minutes and were based upon an interview guide. When in-person (physically or by phone) interviews could not be arranged, due to language facility or time commitments or when requested by participants, the interview guide was provided to the participating DPA to be completed as a questionnaire. Participants were provided with initial information on the purposes and intended use of the interviews, and their desired level of attribution was identified at the start of the interview. Where circumstances allowed and participants were willing, the interviews were recorded and transcribed. Where this was not possible notes were taken by the interviewer. Interview participants were provided with a further opportunity to correct the summary of the interviews.

The interview research process takes participants perspectives as valid perspectives, which can feed into a larger discussion. The interview is a "social event", based on interactions

[9] Given Germany's particular federal model of data protection authorities

between interviewer and interviewee.[10] This means that even where there is potentially disagreement about factual issues, these perspectives are meaningful for the DPAs involved. The semi-structured approach allows for flexibility and adaptation to particular interviewees[11], but also consistency across the six interviewers. As a semi-structured method was used, some DPAs offered opinions or perspectives on issues that were not anticipated in the interview protocol, and at this point it was not possible to confirm if other DPAs would have been in agreement or disagreement with this perspective. Where this is the case, it has been noted in the text. Where we refer to a "majority" of DPAs, we mean a simple majority (over 50 percent), whereas "most DPAs" refers to a large majority. "Nearly all" means there were perhaps one or two dissenting positions, and in these circumstances this has been highlighted. "Some DPAs" is used where more than one or two DPAs expressed a position, but it was not commonly encountered in the interviews.

3. The GDPR and its impacts upon cooperation

The proposed General Data Protection Regulation will make some forms of cooperation between European DPAs a requirement. A key element is included under the duties and powers of supervisory authorities, Article 52, section 1c, which requires that the supervisory authorities "share information and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation" In particular Chapter VII on Co-operation and Consistency contains articles on lead authorities (Article 54a in the Parliament version), mutual assistance (Article 55), joint operations of supervisory authorities (Article 56), the consistency mechanism (Article 57). The interviewers asked participants what impact they envisaged that the passing of the GDPR, and particularly those provisions directly related to cooperation, would have upon their ability to cooperate and co-ordinate with other DPAs.

Most DPAs anticipated a significant, strong impact from the passing of the GDPR in general, and particularly for cooperation between European DPAs. The stance of many DPAs towards the GDPR was optimistic, although often balanced with some caution, or a recognition of additional work that needed to be done, and pending issues that would need to be resolved. Several expressed a feeling of hope in relation to the Regulation. There were however some divergent opinions highly sceptical about the GDPR. Participants reminded us that cooperation between European DPAs was already ongoing through a number of informal mechanisms, and in general this was seen positively, although some participants identified some frustrating experiences they wished to improve (examples included processing communications in minority languages and differences in strategy). All DPAs recognised the need for increased collaboration within the European Union. Several DPAs informed us that they expected the drive to more frequent cooperation would come primarily from both European citizens and business, who would, under the GDPR, have increased expectations

[10] Blakely, Ruth, Elite Interviews, In Laura Shepherd (Ed.), *Critical Approaches to Security: An introduction to theories and methods*, London & New York, Routledge, 2013.
[11] Fielding, N. & H. Thomas, "Qualitative interviewing" in G. Nigel (Ed.) *Researching Social life*, London, Sage Publications, 2001; Rubin, H.J & I.S. Rubin, *Qualitative Interviewing: The Art of Hearing Data*, London, Sage Publications, 1995.

about cooperation and consistency from their interactions with European DPAs, and that this would increase the onus upon DPAs to cooperate. DPAs expected the number of overseas complaints to increase, although this was dependent upon the particular context of the individual DPAs, in relation to their national environment and their relationship with their peers. The presence or absence in a jurisdiction of large multinational corporations engaged in the processing of cross-border data was seen as a significant determining factor in the extent and direction of cross-border complaints. It was suggested that they anticipated that European cooperation would become increasingly routine, and part of the "daily life" of EU DPAs. Other DPAs suggested that increased cooperation would, over time, smooth out and routinise interactions between DPAs, and building upon successful examples and interactions would help to create a culture of cooperation which could improve over time. Additionally, It was suggested that the obligation to cooperate under the GDPR could potentially provide additional weight to requests for cooperation. In general, DPAs believed that increased cooperation under the GDPR would bring an increased administrative burden and may raise resource and capacity issues. Although positive remarks were made by DPAs about the GDPR, one DPA expressed a divergent critical perspective stating that the legal basis of the GDPR would be challenged in the Court of Justice of the EU, and that it would be difficult for small DPAs to implement some of the cooperation mechanisms. There were also concerns that the role of "concerned DPAs" might slow down or potentially block decisions.

Issues to be resolved, and where further work was anticipated, included technical and administrative mechanisms (the actual process of collaboration under the GDPR) and implementing acts, but also the spirit and attitude towards cooperation. The need to find a systematic solution to the issue of multiple working languages was raised by several DPAs. DPAs pointed out that the GDPR would not regulate all forms of cooperation. A number of DPAs offered information on the measures they were taking to prepare for the passing of the GDPR, including actions they would have to take in the leading period after the Regulation was passed, but before it came into force. Other DPAs were waiting for the text of the Regulation to stabilise before putting adaptive measures into place.

3.1 The consistency mechanism

The "consistency mechanism" would be established by Article 57. According to the European Commission, the mechanism is part of a new system for supervision of organisations processing personal data in one or more EU Member States or with a pan-EU impact. It is intended to "ensure coherent application of the rules" and "combines an advisory role for the European Data Protection Board and a role for the Commission".[12] The basic principles of the mechanisms are that DPAs take decisions on cases without an EU-wide impact; where there is an EU impact the European Data Protection Board is engaged and issues an opinion (based on a simple majority). The consistency mechanisms also includes provisions on decisions regarding reasoned objections between DPAs , non-compliance with requirements for mutual

[12] European Commission, "The proposed General Data Protection Regulation: The Consistency Mechanism explained", 06 February 2013, ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm

assistance to be reported to the EPDB, on individual cases and on matters of general consistency.

The DPAs had a range of perspectives upon the consistency mechanism. Some DPAs were unwilling to comment on the consistency mechanisms until discussion in the Council and the trialogue had concluded. It was described by one DPA as "the best possible compromise" and a key source of the need for DPAs to improve their regular communication.

Some DPAs expressed doubt about the mechanism. Particular concerns included uncertainty about how the mechanism would work in practice, the risk of multiple interpretations of the mechanism, the speed of the envisioned process, the clarity of the rules, and in particular the complexity of the current workflow and how this would be understandable by both DPAs, and more significantly, by EU citizens and data controllers. Elements of the consistency mechanism that were seen as needing some work included the integration of the mechanism at the levels of citizens and the time limits for decisions.

A small number of DPAs expressed the need to limit the function of the consistency mechanism to only those cases with a cross-border component. This was linked both to the administrative burden of the mechanism, but also the more political concern of the DPA losing discretion (including discretion to enforce) and leaving room for the effects of national legislation (such as that on access to public documents and transparency laws). There were mixed opinions regarding negotiations in the context of the Working Party on Information Exchange and Data Protection (DAPIX).

3.2 The One-Stop-Shop

Related to the consistency mechanism, the GDPR proposes a "One stop shop" principle, in which only one DPA is responsible for taking legally binding decisions against a company, with that DPA being determined by the company's main establishment in the European Union.[13] The aim of the one-stop-shop principle is to ensure consistent application, legal certainty and reduce administrative burdens.

A key concern raised by a minority of DPAs in relation to the One-Stop-Shop principle was the risk of "forum shopping" on the part of data controllers. It was suggested that controllers might try to avoid enforcement by locating their main establishment in countries with a less onerous enforcement approach. More broadly, several DPAs expressed concern that the one-stop-shop principle should be framed in such a way that it focused upon the exercise of data

[13] See Recital 98 of the European Parliament version of the GDPR, which amends the Commission version from "The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment." to "The lead authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment or its representative. The European Data Protection Board may designate the lead authority through the consistency mechanism in certain cases on the request of a competent authority." European Parliament legislative resolution of 12 March 2014 on the 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 the free movement of such data (General Data Protection Regulation),http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.

protection rights by European citizens, and facilitated the ability of citizens to file complaints in their home jurisdictions. It was suggested that although the model looks potentially complex, this complexity will not be a concern of the citizen or data subject, but rather be handled by the authorities involved.

Challenges related to this principle include communication with citizens and explaining how the principle works and how they can best use it to exercise their rights. Concerns were again expressed regarding language and interpretation requirements (particularly when DPA decisions are challenged or go to court proceedings, which then might have to be conducted across linguistic divides). In a similar manner to the consistency mechanisms, DPAs expressed concerns about the one-stop-shop in relation to jurisdiction disputes and complaints against controllers offering services in only one country, and the ability of appealing against DPA decisions to judges based in foreign countries.

The one-stop-shop principle is an area where several DPAs stated that they were paying close attention to ongoing discussions and dialogue, and some stated that more recent versions of the principle were regarded as more clear, and less problematic than earlier versions. In spite of this, DPAs did express concerns about the practical implementation of the principle.

3.3 The European Data Protection Board

The interviewers asked DPAs for their perspective upon the proposed European Data Protection Board, its implications for cooperation between European DPAs and the impact of the shift from the existing Article 29 Data Protection Working Party to the Board. DPAs expressed some uncertainty about the role, responsibilities, powers, legal standing, and internal decision-making processes of the Board. Discussions on the nature of the EDPB were seen as still ongoing.

A general perspective was that the EDPB would be a positive development. Cooperation under the Article 29 Working Party seemed to be generally well-regarded and DPAs were generally seeking to build upon this. However, some DPAs were cautious about losing some of the strengths of the existing model in the transition to a new way of working.

Coordination, communication and conflict-resolution between DPAs were identified as key roles for the Board. The EDPB was seen as having an increased practical role in relation to handling individual cases. Some DPAs saw an additional role in dealing with the equal implementation of the GDPR across Member States. These tasks were seen as adding to the workload of the EDPB in comparison with the Article 29 Working Party, and as having potential resource implications. The EDPB was seen by one DPA as introducing *collective decision making* for DPAs, in addition to the formulation and expression of collective opinion, as through the Article 29 Working Party.

That the EDPB would have legal personhood, and the ability to issue binding decisions was seen as positive by DPAs. Internal decision making in the board raised the issue of how decisions, the number of which were anticipated to increase with the increased practical (in addition to advisory) role of the board, would be handled. Unanimous decision making was

seen by some DPAs as too cumbersome, and would lead to unworkable blockages. Instead, they advocated majority decision making, although all DPAs who commented on this stressed the need for consensus building efforts and time for discussion. However, several DPAs stated that it was important to achieve a balance between the powers of the Board and the autonomy of national DPAs, as there could be tensions there. The role of the EDPS as the secretariat of the board was questioned, and compared with the potential for the Board to have been constructed as an Independent Agency. Several DPAs commented on the issue of the EDPB having its own budget, with sufficient resources for the various tasks that would be attributed to it. One DPA raised the issue of how the Board would integrate or operate in an international environment, with an increasing number of bodies having some regulatory role, or policy interest in data protection.

Several DPAs emphasised possible implications related to the establishment of the EDPB that would occur at national level. German DPAs, for instance, raised the issue of how to determine voting rights for German DPAs at the state level within the EDPB, an issue which is currently in discussion amongst the affected parties through the German Conference of Data Protection Commissioners.

3.4 The Trialogue

The interview participants were asked if they had any perspective on issues that the collective body of DPAs or individual authorities should attempt to feed into the Trialogue[14] discussion process between the Commission, Council and Parliament before the GDPR could be finalised.[15] Several DPAs deferred on this question, citing a division (either explicitly constitutional or conventional) between lawmaking and enforcement roles, which placed the negotiation process in the hands of Member State representatives. However, the Article 29 Working Party was seen as observing the process, and in a potential position to feed those perspectives shared by DPAs into the Trialogue following a decision by the Council. The working party has subsequently issued such a position reiterating the need that reforms not lower the protections for European citizens.[16] Another DPA informed us that there is clearly scope for DPAs to feed into this process as stakeholders by expressing views to their national governments.

3.5 Information sharing

The proposed GDPR would require DPAs to share “relevant” information with each other. In particular, they face a requirement under Article 52 of the Parliament version to "share information with and provide mutual assistance to other supervisory authorities", and a requirement for lead authorities to communicate relevant information to concerned authorities

[14] Trialogues are informal negotiations between the European Parliament, the Council and the Commission, aimed at reaching early agreement on new EU legislation. The use of the trialogue procedure has been increasing in use, in an attempt to speed up the EU's co-decision process.

[15] There were a smaller number of responses to this question as it was a question that was dropped from some interviews because of time constraints and prioritisation of other lines of questioning.

[16] Falque-Pierrotin, Isabelle, "letter to Ms Ilze Juhansone", Article 29 Data Protection Working Party, Brussels, 17 June 2015, https://privacyassociation.org/news/a/wp29-weighs-in-on-the-gdpr-trilogue-process-2/

in particular cases, and a requirement under Article 55 in relation to providing information to each other relevant to mutual assistance.

We asked the DPAs how their offices would determine what was “relevant” information. From the interviews, DPAs broadly understood the necessity of sharing information with their European peers, and that this would likely increase in some manner under the GDPR.

Several DPAs told us about the various fora in which they shared information with their European peers, in particular the Article 29 Data Protection Working Party and its various sub-groups. Many other fora were also positively mentioned.

With regard to their current status, some DPAs informed us about their ability to share information. Information sharing was done primarily on an informal basis. In the context of the GDPR, some DPAs anticipated continuing with this approach.

For the most part, DPAs suggested that they currently shared information as necessary, and as required for a particular case, in relation to the context of that case. There was therefore not a standard set of information that was exchanged in most cases. Relevancy was determined through contextual criteria, ranging from such as "all pieces of information that are useful in assessing the issue at hand" to "all relevant information need to take the appropriate procedural and material measures in order to solve a case" and "the information which we consider as necessary for adoption of a decision". Relevancy was determined by informing a DPA, with the possibility of negotiation and discussion if the receiving DPA felt there was some information missing.

In the context of a case referred to another DPA due to the geographical location of a data controller, DPAs stated that they would pass on all information required for the investigation, but would expect to remain informed by the investigating DPA in order to be able to inform the data subject/complainant in turn.

Some concerns were raised about the sharing of personal data between DPAs in the context of an investigation. Some DPAs identified legal barriers around confidentiality that prevented them from sharing information. Some DPAs identified restrictions on sharing information with DPAs outside the EU and that this was at least one factor in their non-participation in GPEN (the Global Privacy Enforcement Network, see below). However, others (who themselves did not identify a barrier) suggested that such concerns might be overstated and that in their experience, information that needed to be shared for cross-border investigations was generally not the personal data involved in the case, but rather information on the nature of the incident, circumstances, and the opportunities for cross-border working, including identifying the jurisdiction in which a data controller is located. However, some DPAs may be bound to secrecy according to national secrecy legislation, particularly in relation to functions of audit and inspection, that will not be altered by the passing of the GDPR. One DPA suggested that due to the GDPR (consistency mechanism and one-stop shop, and a EDPB with binding decisions) meaning that European DPAs would start acting as, in a certain sense, a "big, single DPA" that national level confidentiality requirements might have to be interpreted in this manner to allow sharing of confidential information within this

group. Others suggested that the exchange of confidential case information between DPAs for cases with cross-jurisdictional elements was part of their operational procedure. DPAs stressed that the issue of sharing confidential information is still pending and awaiting resolution in the framework of the GDPR. Also, some DPAs underlined that in the meantime this has originated constitutional courts cases which are under judicial review.

One DPA highlighted the need to keep information sharing to actual cross-border cases, and that in this context, the determinant of relevancy was the information required to bring about a cross-border resolution to a case. DPAs in general seemed very willing to share anonymised versions of their cases, post-investigation, and investigations with their peers, particularly in closed environments.

4. Developing cooperation frameworks

4. 1 Structured information exchange

We asked DPAs if they would value a structured system for the exchange of information with other DPAs. If so, we asked about the requirements for such a system and what types of information would they be most interested to share. Opinion was somewhat divided on this perspective. Several DPAs reiterated that they were broadly supportive of the idea of sharing information with their European peers. In addition, several DPAs were supportive of the concept of a structured system for doing this. It was seen as useful, increasing efficiency and helpful for parties to understand each other better.

Some DPAs expressed that a structured system of some form was a necessity. Drivers for the creation of a structured system for information exchange included the anticipated increase in information sharing and collaborative working arising from the GDPR, the pursuit of efficient modes of working, or the alternative of dealing with 29 different sets of practices, requirements and document templates. Several DPAs expressed that some form of structure for information exchange would be beneficial or convenient, and that this might reduce communication workloads by removing unnecessary communication. Such a system might include key categories of information and serve as a checklist or reminder for DPAs as to the types of information that are commonly needed, serve as an "outer limit" for focusing information, and prevent the "blur" of unstructured information. The types of information that DPAs anticipated sharing (or were seeking to gain access to) included plans and intentions, case law, decisions, experiences and best practices, informal thinking, opinions, and requests for opinions.

Some DPAs were less supportive. The exchange of information through current "unstructured" methods was seen as adequate and the lack of a structured system was not the key barrier to DPA cooperation and coordination. Clever and well designed systems for information exchange would likely not harm DPA cooperation, but if their absence was not the key barrier or challenge, then they would have little positive impact. Even supporters acknowledge that a system would have to have significant flexibility in order to cope with the various ways that DPAs might have to work together and the diverse types of investigation or cases that they would have to deal with. This meant it would be difficult to specify in advance

many elements of the structure. DPAs also acknowledged that there were limits on the types of information that could be shared. As with many other areas of coordination between DPAs, the issue of language was raised in this context: which language(s) would a structured information exchange system support? Active and ongoing translation would be an expensive cost.

DPAs suggested that pre-agreement on the way that information would be exchanged would be necessary even in the absence of a formal structured system. One suggested that shared principles and purposes for communication and information exchange should be established between European DPAs before any form of technological solution was developed to support this.

DPAs suggested potential ways in which a system might operate or sources of inspiration and learning for the design of such a system. These included: Some kind of dashboard functionality for understanding ongoing investigations, potentially based upon that developed by the Belgian DPA for the Google Spain judgement; the national intelligence model used by Interpol for sharing information on international criminal cases (appropriately adjusted for the activities that DPAs conduct) where shared intelligence is categorised and assessed under a number of categories; existing discussions between the Nordic states, virtual working space and collaboration tools; an internet database or extranet; and in one suggestion, that document templates, rather than any additional form of software or communication technology, would be the most appropriate solution.

DPAs expressed mixed perspectives upon the existing tool the Communication and Information Resource Centre for Administrations, Businesses and Citizens (CIRCABC)[17]. One DPA felt that the tool was good, but that it was currently under-used. Others expressed doubts, particularly that the tool was not designed for this purpose, was not controlled or owned by DPAs, and was not integrated with the day-to-day workflows of any authority.

Barriers to the use of any such system included that it was not a priority topic and would attract limited attention, logistical issues including financial and organisational barriers, legal barriers of various severity in national legislation, a limit upon sharing information outside of the EU, and the uncertainty that the GDPR would provide sufficient legal gateways around national limitations upon the sharing of confidential information. Such a system would also have to be more effective and efficient than the exchange of specific, focused email between individual officers in different DPAs. Such a system would need to pass an efficiency test, with many other competing priorities likely to overtake putting information onto a system that was too onerous to use. Even CIRCABC seems to suffer in this regard.

4. 2 Sharing best practice

[17] CIRCABC is a tool for the distribution and management of documents across multiple languages and with document control. It allows users to create collaborative online working spaces, and share information and resource. It is open source software and can be downloaded and used by anybody. European Commission, *CIRCABC 3.6 User Guide, Version* 2, 22 January 2014, https://circabc.europa.eu/d/a/workspace/SpacesStore/1baaac9f-6c08-406c-a0c1-d34262bbe0ba/CIRCABC_User_Guide.pdf

DPA interviewees were asked how they currently share information on best practice with other DPAs. The report "Co-ordination and Co-operation between Data Protection Authorities" from the first phase of the PHAEDRA project provided an overview of this area[18], and the answers received to this question support the findings there. Sharing of best practice occurs through various mechanisms and forums, including international conferences, working groups, the case handling workshops and associated network, joint inspections and common audits, bilateral discussions, staff exchanges and visits, asking direct questions of other DPAs on topics of shared interest, task forces.

DPAs identified different channels as being the best source for the exchange of particular types of intervention, in particular through the interaction of different types of specialist staff, for example Commissioners, lawyers, and IT experts. There is some doubling-up of networks (for example, the case handling network and the Article 29 Working Party have very similar membership).

DPAs expressed clear appreciation for the willingness of their European colleagues to relatively freely exchange experiences in response to direct questions about experiences, positions and activity from their peers. DPAs acknowledged that the experiences and decisions of their peers needed to be understood in the context of national contexts and in particular in light of national legislations, but several DPAs said that they gained very valuable perspectives from these exchanges. In addition, some DPAs stated that they preferred to share these experiences in interactive sessions with their peers, where questions could pass back and forth and details be discussed.

4.3 A standardised EU approach to "requests for assistance"

DPAs were asked their opinions on desirability and feasibility of standardising the way that DPAs approached their European counterparts with requests for assistance. Several DPAs stated that such a standardised approach was a necessity. Others expressed that a standardised approach to the presentation of requests for assistance would be useful and that it could facilitate cooperation and coordination. A standardised approach might allow DPAs to make better informed decisions about the requests being presented to them, and allow for clearly setting the parameters of any joint or transferred investigation and for organising the division of work (based upon, for example technical or investigative experience), as well as increasing the speed and efficiency of communication. The awareness that similar procedures were being followed was seen as useful. Others contextualised this form of operational cooperation against a background of global data protection issues that did not follow national borders, and the need to provide high quality and effective services to both data subjects and data controllers.

Any standardised approach to requests for assistance was seen as needing clear and simple rules, to be agreed collectively by EU DPAs, and finding a resolution to several practical issues, particularly in relation to language and translation. Such a system, we were told, should also retain some space for information that did not fit within the structure, but that

[18] Barnard-Wills & Wright, 2014, Op.cit.

nevertheless needed to be exchanged as part of a request. The approach must therefore have some capacity to respond to the particular nature of a case. Standardised templates for requests for assistance would have to be well developed, and if so, they would serve as a reminder to include appropriate information. Information that was identified as an appropriate part of such a structured approach included the subject of the complaint, the technical circumstances, any other data subjects affected by the breach, and involvement of an IT or manual system. However, some DPAs suggested that it was the attitude to cooperation that was most important, regardless of the approach or template used in practice.

One perspective was that the current system of bilateral requests, often formal written memos from one DPA to another, worked acceptably well for the relatively low volume of cross-border complaints received by DPAs. Some DPAs provided details of the Memoranda of Understanding (MoU) that they had established with particular peers, which provided some structure to their interaction and cooperation. One DPA expressed concern that a standardised approach might actively hinder and limit cooperation and communication that was already occurring in less formal ways.

It was suggested by one DPA that it could be useful to take the Google Spain judgement recommendations of the Article 29 Working Party as a reference model[19]. DPAs provided examples of systems in different fields that could be used as examples and inspiration for data protection. These included the field of asylum claims, the system for passing on fines for violations of traffic rules between different EU states, criminal law cooperation in the Council of Europe, and the well-established tradition of mutual legal assistance. These systems were not seen as perfect, but sufficiently functional to learn from.

4.4 The role of the European Commission

DPAs were asked what role (if any) would they want to see the European Commission take in the development of a co-operation framework for DPAs, and if coordination should be a DPA "leadership role". The majority of DPAs interviewed suggested that the leading role in cooperation and coordination between data protection authorities should be played by the authorities themselves, in order to maintain their independence and effectiveness. DPAs were also seen as the site of knowledge and experience on cooperation and on enforcement. This extended to the development of specific frameworks and methodologies for cooperation between them. Coordination between DPAs was seen as best occurring through bilateral or multilateral arrangements between the DPAs themselves, including the Article 29 Working Party and EDPB, whilst DPAs were seen as the actors who would have to prose and develop any cooperation framework they would use.

[19] These recommendations included common criteria to be used by data protection authorities when handling complaints. See Article 29 Data Protection Working Party, *Guidelines on the implementation of the court of Justice of the European Union judgment on the "Google Spain and inc V. Agencia Espanola de protection de datos (AEPD) and Mario Costeja Gonzalez" C-131/12,* WP225, 26 November 2014, *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf*

In particular, the European Commission was seen as having no competence in data protection enforcement. The role of the European Commission was therefore, for the most part, seen as facilitating activity by the DPAs, through the provision of resources, and tools. In this context there was criticism of the number of delegated acts foreseen in the GDPR, and another anticipated that the passing of the GDPR would increase the influence and powers of the Commission in this area. Some DPAs saw a role for the Commission in detailing implementing acts of the Regulation.

Suggested activities that the Commission could undertake to better support cooperation and coordination between DPAs included the provision of language support and translation services, the provision of research and background information, technical infrastructure (as with CIRCABC), technical assistance, support for an alerting tool, administrative tools. Support from the Commission was seen as potentially important during the leading period between the Regulation passing and it coming into force. According to several DPAs support from the Commission should be requested by the DPAs as required. One DPA did suggest that the Commission might have some role in developing standard forms and templates, in multiple languages. Another suggested that the Commission might be able to play a role in evaluating the extent to which different DPAs met the various requirements of Regulation, and could express opinions on the extent to which DPAs had sufficient IT resources and human resources. This authority also suggested that the Commission had a role to play in observing and coordinating on international political issues (such as trans-Atlantic discussions about Passenger Name Records) which are more political than they are legal or judicial, and maintaining awareness. Neither of these DPAs saw a role for the Commission in day-to-day cooperation or work of DPAs.

In discussing leadership roles more broadly, DPAs raised the issue of "lead DPA" in investigations,[20] and the way in which the EDPB could play a role in determining lead DPA and main establishment when there were disagreements.

4.5 Common approach to complaint handling

The interviewers asked the DPAs if they considered the development of a common EU approach to complaint handling to be desirable and feasible. Several DPAs expressed support for a common approach to complaint handling, believing that it was both necessary and desirable. Some DPAs expressed the belief that a common approach to complaint handling would be the eventual result of the GDPR, as these provided a drive towards harmonisation. Particularly the one-stop-shop and consistency mechanisms were seen as driving towards harmonisation in complaint handling in order to treat European citizens fairly and to deal with increasing international complaints.

Others were significantly more cautious. Some were concerned about independence and over-regulation of their activities, and believed a common approach would require careful consideration. The GDPR was described as having made the decision to retain national DPAs, who had to interact in specific national contexts, preventing the possibility of a

[20] The concept of the "Lead DPA" envisaged in the Regulation

common approach. One DPA highlighted the multiple ways in which they could receive and accept a complaint (with about half not being received through their own standard forms). The complexity of any standardised process was also raised as a potential barrier. Several DPAs wanted to limit a common approach to complaint handling to cases with a cross-border element. Others suggested that sharing the results of complaint handling, and the process of learning from similarities and differences, would be more effective way to spend effort than trying to standardise the procedure.

Even those DPAs who were supportive of a common approach (or believed it an eventual requirement) acknowledged the difficulty of reaching a common approach given the variety in DPA practice, administrative and other laws in different Member States, different requirements and competencies of DPAs, applicable deadlines, information sharing, sanction powers, and differences in culture and regulatory approach. They commented that such an approach would have to take into account and be sensitive towards these differences. Therefore, a common approach to complaint handling would, according to some DPAs, require additional clarification and harmonisation following the GDPR. One DPA suggested that it would first be necessary to understand how complaints are currently handled across the Member States, analyse these and identify models that are the best, or that could work in a better way.

4.6 Alerting tools

DPAs were asked if the Global Privacy Enforcement Network (GPEN)[21]alerting tool was sufficient for their communication and alerting needs or would they prefer to see another alerting tool, e.g., from the Article 29 Working Party (or EDPB) or from the International Conference of Privacy and Data Protection Commissioners?

Several DPAs informed us that they did not participate in GPEN. For some this was a result of a legal requirement, for others it was a political matter (for example related to maintaining independence), and for a third group, they had not yet pursued membership. Several described a limited participation (participating in sweeps, but not becoming members, or using GPEN for exchange of knowledge and experience rather than organising cooperation, being a member but not participating in much activity because of their specific national data protection context). Amongst the non-members, there was awareness of the existence of an alerting tool, but some uncertainty about its functions and mode of operation.

[21] For an outline of GPEN's composition and activity, please see PHAEDRA project report *Coordination and Cooperation between Data Protection Authorities*, 30 June 2014. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf GPEN Alert "is intended to be a secure Internet-based platform that will allow GPEN members to alert other members about investigations and find out whether other members are investigating the same company or practice. GPEN members from British Columbia, Canada, the United Kingdom, Norway, Australia, Ireland and New Zealand pledged significant financial support to the development of the system. GPEN members participated in several exchanges of proposed documentation, culminating in a "near final" version of the GPEN Alert documents being distributed in November of 2014." - Stewart, Blair, "Big Year for Global Privacy Enforcement Network:GPEN releases 2014 annual report" 1 April 2015, https://www.privacyenforcement.net/node/513

Some of these DPAs expressed a preference for a tool without links to the United States (GPEN's information technology is provided by the US Federal Trade Commission) or other national control, and in this case an international or European body was the preferred host for an altering tool. GPEN was not seen as a sufficient stand in for European alerting mechanisms, even if more European DPAs would join. Others suggested that the emergence of parallel models with different membership, which could be alerted on particular issues of relevance was the best approach.

Whilst some DPAs were a little sceptical about the benefits and capacity of the GPEN alerting tool, and warned us against reading too much functionality into something quite technologically simple (essentially the "alerting tool" is a newsletter function). Additionally, others suggested that most information exchange occurred through phone calls and face-to-face discussions at conferences rather than through any structured tool, and that there was real benefit to this "coffee break" interaction, even if there was a need for formalisation of the organisation of cooperation. The simplicity of the GPEN method was seen as a potential positive aspect for some DPAs. Some were uncertain about the extent to which an alerting tool at the level of functionality that exists within GPEN might not just duplicate channels of communication which already exist within and between the members of the Article 29 Working Party.

Beyond GPEN DPAs provided examples of practice in consumer protection alerts, and informed us about the development of a cooperation framework within the Spring Conference and the creation of an Article 29 subgroup on enforcement cooperation. The latter was seen as a very positive step for increasing practical cooperation.

There was general, if somewhat muted support for an EU equivalent of the GPEN alerting tool, although some DPAs were unsure about the nature of the GPEN tool, and the capabilities it offered. An alerting tool offered possibilities to some DPAs interviewed. This included improving communication in and around joint actions. DPAs with positive perspectives upon the GPEN tool spoke about the possibility of a parallel mechanism under the EU Regulation, and that both of these frameworks could potentially engage in mutual learning, and avoid reinventing the wheel. Other DPAs simply suggested they would use any effective tool that was developed.

Some DPAs highlighted diversity, stating that they did not want to rely on a single alerting tool, and that access to multiple alerting processes might instead be beneficial. Other DPAs presented an opposed perspective, warning against the multiplication of fora and platforms resulting in a decrease in efficiency, with DPAs have to enter the same (or subtly different) information into several different platforms. These DPAs instead preferred a single harmonised platform for information exchange. Another stated that they would need to conduct an in-depth analysis to determine which are the best tools. It was suggested that the onus sat with the communicating party to assess how they needed to make any particular piece of information visible and who they wanted to see it.

One DPA suggested that many of the cooperative activities anticipated under the GDPR (mutual assistance, the consistency mechanism, one-stop-shop and joined inspections) could be interpreted as alerting tools. Others suggested that such communication mechanisms would likely have to be developed to put the various provisions of the GDPR into practice.

Requirements for an alerting tool that emerged during the interviews included: that it ideally be automated, quick, efficient, and contain the relevant information for an organisation to make informed decisions about if and how to cooperate. Barriers identified included the capacity and capability of organisations to respond to alerts, and the way that alerts might integrate (or not) with existing work practices within DPAs.

4.7 Budgets for Cross border investigations

DPAs were asked if they were asked to participate in an investigation by another EU DPA, would they have a budget for this? In this context we considered scenarios where a DPA might be asked to either provide information to an investigation (for example, investigating a local subsidiary data processor) or asked to take on the lead role in an investigation when a data controller's main establishment was in their jurisdiction.

Many DPAs said that participating in an investigation with or at the request of another DPA would not pose a budgetary problem or that budgets would not pose an obstacle to responding to such a request. Some DPAs in this position highlighted other cooperation issues (for example coherence and consistency) as more significant than budgetary and financial considerations. Particularly, responding to requests for information or perspectives were not dealt with in terms of their budgetary implications.

Other DPAs told us that their current budgetary arrangements did not contain any provision for cross-border or joint investigations. Some said that the budget could be found for such participation, but that it would require some re-prioritisation of other activities and therefore some careful consideration. Some DPAs anticipated shifting a proportion of their budget to explicitly cover such costs post-GDPR, but that such requests might currently cause a problem.

Some DPAs told us about legal requirements as part of their foundational legislation that required them to investigate all complaints put to them, and that they therefore could not distinguish legally between a complaint put to them by a data subject, or an issue brought to their attention by a fellow DPA. In a similar manner, one DPA suggested that although there was no specific budget for coordination in this respect, they expected properly organised cross-border cooperation to actually reduce their investigating costs.

DPAs did identify potential budgetary issues that would arise with the anticipated increase in cross-border cases under the GDPR. Some told us about their intention to seek an increased budget with the passing of the GDPR. The GDPR contains provisions (see Recital 94 and Article 47) that Member States should provide national DPAs with the resources necessary for cooperation, but DPAs expressed that the exact meaning of this, and how it would be interpreted by national governments was currently unclear (some DPAs were more confident

than others in this regard). The question of some mechanism or agreement on cost sharing or reimbursement was raised, in order for larger and better resourced DPAs to support their smaller partners in investigations, as well as the possibility of recouping money from investigated data controllers (not yet finalised in the GDPR). Cross-border agreement on the distribution of any revenue from increase fines would also have to be achieved. Translation costs were identified as an element of cooperation costs.

One DPA raised the issue of secondment efforts where a member of staff from one DPA might be seconded to another support of particular investigations, and that this would require an appropriate budget.

5. Conclusions

Most DPAs anticipated a significant, strong impact from the passing of the GDPR in general, and particularly for cooperation between European DPAs. The stance of many DPAs towards the GDPR was optimistic, although this was often balanced with some caution, or a recognition of additional work that needed (and needs) to be done, and pending issues that would need to be resolved. In general, DPAs believed that increased cooperation under the GDPR would bring an increased administrative burden and may raise resource and capacity issues. All DPAs interviewed recognised the need for increased collaboration within the European Union (which was seen by some as critical, given that a spirit or attitude of cooperation may be as important as specific legal provisions for cooperation). Several DPAs informed us that they anticipated the GDPR reforms to act as a driver for more frequent cooperation. This differs from our starting assumption that resource issues and the desire to avoid duplication of effort in enforcement would be primary drivers for cooperation and coordination.

The GDPR reform process is still ongoing. The first Trialogue sessions have commenced at the time of writing. There are ongoing discussions on consistency mechanism, one-stop shop and the legal identity, powers and role of the EDPS. There are still things to be decided, and there are still things to be worked out in practice. A still pending issue worthy of further attention is how practical cooperation required by the GDPR particularly through the consistency mechanism, one-stop-shop and the EDPS will be resolved in practice. For example, what will become normal practice for concerned DPAs involved in investigations? What time limits will be considered acceptable in investigations? It may be the case that these norms emerge amongst the community of European DPAs over time, through their experience in this type of cooperative activity. The extent to which the GDPR will harmonise data protection in the EU is still debated. Some DPAs interviewed expressed opinions that the Regulation's provisions would mean European DPAs had equivalent powers and roles, reducing the diversity of national implementations of data protection law, in effect creating a single regime of data protection. Others instead expressed the belief that there would still remain differences in national practice and particularly in both culture and strategy, as well as differences in size, resources, experience and economic context in which they were required to operate as a regulator. A requirement emerging from this may be the need to better

understand where there will be remaining differences in areas not covered (and therefore not harmonised) by the GDPR.

Related to this is a practical debate about the extent to which structure and formalisation can contribute to more effective cooperation and coordination between European DPAs. For a minority of DPAs, the creation of structure systems for information exchange, shared complaint handling strategies, templates, forms, alerting systems, etc. were likely to be necessary given the scale of cooperation under the GDPR. For another minority, such systems were seen as problematic, in that they either reduced the operational flexibility of DPAs and their ability to respond to the particular context of a particular case, or they believed that agreement on such structures would not be possible given the remaining diversity between DPAs, even under the GDPR. For most DPAs structure and formalisation could be potentially helpful in various areas, either increasing efficiency, serving as a check or reminder for processes, and increasing harmonisation. Many reminded us that structured systems would always need to be flexible enough to cope with unanticipated events and requirements.

Key challenges for DPAs include maintaining legitimacy, freedom of action and ability to determine their own strategies and methods, and ability to take what they see as appropriate measures, whilst maintaining coordination and consistency with their peers. Maintaining legitimacy includes concerns about their independence, their relationship to the EDPS and the Commission, avoiding reliance on third party tools and networks.

Language differences remain a key topic of discussion in these interviews, as has previously been identified.[22] Problems raised by language emerged in the interviews in relation to the exchange of information, communication systems, requests for assistance, repositories of decisions, public communication, and dealing with the one-stop-shop. Whilst DPAs generally felt able to communicate with their peers, either with English as a lingua franca or a set of commonly used and known European languages, communication with and from the public in different countries posed a greater challenge, as did the translation of decisions and legal documents in investigations and court cases. Translation imposes resource questions and there was uncertainty about the source of the required resources, and who should carry the cost. Working in common or shared languages, and making a decision about which to focus upon is a highly political issue. Some DPAs looked to the Commission for support in this area. The Commission has experience in working across 24 official EU languages and has one of the largest translation services in the world.[23] Further research might understand the real extent of this problem in practice, and the number of languages required for effective cooperation.

Tools, (including communication, information exchange, alerting tools and systems for structuring requests) were seen as generally useful, but not the limiting factor for cooperation.

---

[22] Wright, David, David Barnard-Wills & Inga Kroener, *Findings and Recommendations*, PHAEDRA project Deliverable 4, Brussels, January 2015, http://www.phaedra-project.eu/wp-content/uploads/Findings-and-recommendations-18-Jan-2015.pdf, p.21

[23] http://ec.europa.eu/languages/policy/linguistic-diversity/official-languages-eu_en.htm

There are some existing tools (and phone calls, emails, and face-to-face meetings should not be discounted in DPA cooperation) even when these have limited technical functionality. Tools might be better designed to fit into operational processes, and the area of information repositories certainly attracted some support. Like any organisations, DPAs have staff turnover, and experience and knowledge that is distributed amongst a peer group can potentially be either permanently lost, or temporarily disconnected from that network by personnel changes. Repositories for storing this information (decisions, opinions, experiences, powers, but also contact information and job responsibilities) and making it more easily searchable are desirable. Such repositories also allow for the potential to avoid the duplication of information-gathering requests and efforts.

These interviews suggest there is a community of EU DPAs with sufficient shared perspectives that it is possible to talk about an EU DPA perspective, although there are of course still differences of focus, position and strategy. This community is collectively and individually preparing for changes in the way that it operates due to data protection reform, and does have a number of options and pathways open to it. The period following the eventual passing of the GDPR is likely to see further working out of these cooperative relationships, and the development of further institutionalised measures in response. How effective these measures will be is open to further investigation.

Acknowledgements

This article is based upon research conducted as part of the PHAEDRA II project ("Improving practical and helpful cooperation between data protection authorities" and the article is possible due to the assistance and contribution of all project partners. The project is co-funded by the European Union and the Fundamental Rights and Citizenship Programme (JUST/2013/FRAC/AG6068), however the contents of this article are the sole responsibility of the authors and cannot be taken to represent the views of the European Commission. More information on the project can be found at http://www.phaedra-project.eu/. In addition to the authors, interviews were also conducted by Dariusz Klosa, Antonella Galetta (LSTS VUB), Pawel Makowski, Beata Batorowicz, Urzula Góral (GIODO), and Artemi Rallo (UJI). Beatriz Thomas and Rosario Garcia (UJI) reviewed earlier drafts. Finally, the authors would also like to thank all the representatives of EU data protection authorities that participated in the interviews.

References

Article 29 Data Protection Working Party, Guidelines on the implementation of the court of Justice of the European Union judgment on the "Google Spain and inc V. Agencia Espanola de protection de datos (AEPD) and Mario Costeja Gonzalez" C-131/12, WP225, 26 November 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

Barnard-Wills, David, & David Wright, Co-ordination and Co-operation between Data Protection Authorities, Workstream 1 Report, PHAEDRA Project, 1 April 2014, Revised 30 June 2014. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf

Bennett, Colin & Charles Raab, The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, Cambridge MA & London, 2003.

Blakely, Ruth, Elite Interviews, In Laura Shepherd (Ed.), Critical Approaches to Security: An introduction to theories and methods, London & New York, Routledge, 2013.

Bygrave, Lee A., Data Protection Law. Approaching Its Rationale, Logic and Limit, Kluwer Law International, The Hague / London / New York, 2002

Costa, Luiz & Yves Poullet, *Privacy and the Regulation of 2012*, *Computer Law and Security Review*, 28, 2012, pp.254-262.

Dean, Mitchell, Governmentality: Power and Rule in Modern Society, 2nd Edition, London, Sage, 2010

De Hert, Paul, Vagelis Papakonstantinou, David Wright & Serge Gutwirth, "The proposed Regulation and the construction of a principles-driven system for individual data protection", Innovation: The European Journal of Social Science Research, Vol.26, No.1-2, 2013, pp.133-144.

European Commission, "The proposed General Data Protection Regulation: The Consistency Mechanism explained", 06 February 2013, ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm

European Parliament legislative resolution of 12 March 2014 on the 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 the free movement of such data (General Data Protection Regulation),http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.

Falque-Pierrotin, Isabelle, "letter to Ms Ilze Juhansone", Article 29 Data Protection Working Party, Brussels, 17 June 2015, https://privacyassociation.org/news/a/wp29-weighs-in-on-the-gdpr-trilogue-process-2/

Fielding, N. & H. Thomas, "Qualitative interviewing" in G. Nigel (Ed.) Researching Social life, London, Sage Publications, 2001.

Kuner, Christopher, "The European Commission's Proposed Data Protection Regulation: a Copernican revolution in European Data Protection Law, *Privacy and Security Law Report*, The Bureau of National Affairs, 02/06/2012

OECD, Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, Paris, 2007, http://www.oecd.org/internet/interneteconomy/38770483.pdf

Newman, A., Protectors of Privacy: Regulating Personal Data in the Global Economy, Ithaca, NY, Cornell University Press, 2008.

Raab, Charles, "Information Privacy: Networks of Regulation at the Subglobal level", Global Policy, Vol.1, No. 3, October 2010, pp.291-302

Raab, Charles & Paul de Hert, "Privacy actors, performances, and the future of privacy protection in Serge Gutwirth, Yves Poullet, Paul de Hert & C. de Terwange & S. Nouwt (Eds), Re-inventing data protection?, Dordrecht, Springer, 2009

Rubin, H.J & I.S. Rubin, Qualitative Interviewing: The Art of Hearing Data, London, Sage Publications, 1995.

Stewart, Blair, "Big Year for Global Privacy Enforcement Network:GPEN releases 2014 annual report" 1 April 2015, https://www.privacyenforcement.net/node/513

Schütz, P., "Comparing formal independence of data protection authorities in selected EU member states"., Conference Paper for the 4th ECPR Standing Group for Regulatory Governance Conference 2012.

Thatcher, Mark, "Regulation after delegation: Independent Regulatory Agencies in Europe", Journal of European Public Policy, Vol. 9, No.6, 2002, p. 956

Wright, David, David Barnard-Wills & Inga Kroener, Findings and Recommendations, PHAEDRA project Deliverable 4, Brussels, January 2015, http://www.phaedra-project.eu/wp-content/uploads/Findings-and-recommendations-18-Jan-2015.pdf

Wright, David & Kush Wadhwa, "Cooperation and Coordination viewed by supervisory authorities themselves: Result of the PHAEDRA surveys" in Paul De Hert, Dariusz Kloza & Pawel Makowski (eds.) *Enforcing Privacy: Lessons from current implementations and perspectives for the future*, Warsaw, Wydawnictwo Sejmowe, 2015. http://www.phaedra-project.eu/wp-content/uploads/phaedra1_enforcing_privacy_final.pdf

David Barnard-Wills*,

Trilateral Research

Crown House, 72 Hammersmith Road, London, W14 8TH

david.barnard-wills@trilateralresearch.com

+ 44 (0)20 7559 3550 (tel)

+44 (0)20 7559 3551 (fax)

Paul De Hert

Vrije Universiteit Brussels (LSTS)

Tilburg University (TILT)

Law Science Technology & Society (LSTS)
Building B, room 4B317
Vrije Universiteit Brussel
Pleinlaan 2
B-1050 Brussels
Belgium

+32 2 629 24 60

fax +32 2 629 26 62

paul.de.hert@vub.ac.be

Cristina Pauner Chulvi

Universitat Jaume I

Universitat Jaume I CIF: Q-6250003-H Av. de Vicent Sos Baynat, s/n 12071 Castelló de la Plana, Espanya

pauner@uji.es