PHAEDRA II - IMPROVING **P**RACTICAL AND **H**ELPFUL CO-OPER**A**TION BETW**E**EN **D**ATA P**R**OTECTION **A**UTHORITIES II
http://www.phaedra-project.eu/

Authorities' views on the impact of the data protection framework reform on their co-operation in the EU

Deliverable 1

version 1.0
London – Brussels – Warsaw – Castellón, July 2015

Project co-funded by the European Union under the Fundamental Rights and Citizenship Programme (JUST/2013/FRAC/AG/6068).

A report prepared for the European Commission's Directorate-General for Justice (DG JUST).

The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Authors	
Name	**Partner**
David Barnard-Wills	Trilateral
David Wright	Trilateral

Interviewers	
Name	**Partner**
David Barnard-Wills	Trilateral
Artemi Rallo	UJI
Dariusz Kloza	VUB-LSTS
Antonella Galetta	VUB-LSTS
Beata Batorowicz	GIODO
Paweł Makowski	GIODO

Internal Reviewers	
Name	**Partner**
Antonella Galetta	VUB-LSTS
Dariusz Kloza	VUB-LSTS
Rosario Garcia	UJI
Cristina Pauner	UJI
Beatriz Tomás	UJI
Beata Batorowicz	GIODO

Institutional Members of the PHAEDRA II Consortium	
Member	**Role**
Vrije Universiteit Brussel (VUB) Research Group on Law Science Technology & Society (LSTS)	Project Co-ordinator
Trilateral Research & Consulting (TRI)	Partner
Bureau of the Inspector General for Personal Data (GIODO)	Partner
Jaume I University (UJI)	Partner

Contents

Executive summary

The main goal of the PHAEDRA II project – or "Improving Practical and Helpful co-operAtion betweEn Data pRotection Authorities II" (2015-2017) – is to identify, develop and recommend measures for improving practical co-operation between European Data Protection Authorities (DPAs). PHAEDRA II is focused on the challenges for co-operation arising from the reform of the European data protection framework and from the EU framework currently in force. The project is tackling three of the biggest challenges facing European DPAs: ensuring consistency, sharing different types of information (including confidential information) and co-ordination and co-operation regarding enforcement actions. This report provides the findings from a series of interviews with senior representatives of EU DPAs in April-May 2015. Topics covered in the interviews include the main developments of the GDPR, including the consistency mechanisms, one-stop shop, European Data Protection Board, and their impact on cooperation between EU DPAs; challenges to co-operation and co-ordination between EU DPAS; cooperation and coordination regarding enforcement and the perspectives of the DPAs on the activities envisaged within the PHAEDRA II project - a repository of key DPA decisions, investigating the feasibility of a common approach to complaint handling, mapping enforcement powers and technology watch activities.

Most DPAs anticipated a significant, strong impact from the passing of the GDPR in general, and particularly for co-operation 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. All DPAs interviewed recognised the need for increased collaboration within the EU (which was seen by some as critical, given that a spirit or attitude of co-operation may be as important as specific legal provisions for co-operation). Several DPAs informed us that they anticipated the GDPR reforms to act as driver for more frequent co-operation. A still pending issue is how practical co-operation required by the GDPR, particularly through the consistency mechanism, one-stop-shop and the EDPB will be resolved in practice. Further, the extent to which the GDPR will harmonise data protection in the EU is still debated.

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 co-ordination and consistency with their peers. a practical debate about the extent to which structure and formalisation can contribute to more effective co-operation and co-ordination between European DPAs. For a minority of DPAs, the creation of structured systems for information exchange, shared complaint handling strategies, templates, forms, alerting systems, etc. were likely to be necessary given the scale of co-operation 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. Language differences, and the way that these can be resolved in practice, were also a common topic of discussion. Tools – including communication, information exchange, alerting tools and systems for structuring requests – were seen as generally useful, but not the limiting factor for co-operation. The report provides an overview of the perspectives of EU DPAs at this stage in the data protection reform process and in particular of areas where further work is required and identifies issues that will need to be debated in more detail.

List of abbreviations

DPA	data protection authority
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
GDPR	General Data Protection Regulation
GPEN	Global Privacy Enforcement Network
PC	privacy commissionner
PIA	privacy impact assessment

1 Introduction

1.1 The PHAEDRA II project

The main goal of the PHAEDRA II project – or "Improving Practical and Helpful co-operAtion betweEn Data pRotection Authorities II" (2015-2017) – is to identify, develop and recommend measures for improving practical co-operation between European Data Protection Authorities (DPAs). The PHAEDRA II project represents the second phase of the PHAEDRA project.[1] The first phase examined co-operation and co-ordination mechanisms, approaches and legal frameworks between data protection and privacy authorities around the world. PHAEDRA II is focused on the challenges for co-operation arising from the reform of the European data protection framework and from the EU framework in force. The project will tackle three of the biggest challenges facing European DPAs: ensuring consistency, sharing different types of information (including confidential information) and co-ordination and co-operation regarding enforcement actions.

The purpose of this report is to provide the consortium stakeholders with the findings from a series of interviews conducted by the project partners.

The report sets out the methodology, the findings from the interviews and some considerations for the PHAEDRA II project as it continues.

1.2 Methodology

To compile this report, the PHAEDRA II consortium partners (Vrije Universiteit Brussel, Trilateral Research & Consulting, Generalny Inspektor Ochrony Danych Osobowych (GIODO) and Universitat Jaume I) conducted a series of semi-structured interviews with senior representatives of European data protection authorities between April and May 2015. These interviews lasted between 30-45-75 minutes and were based upon an interview guide developed by the consortium. The interview guide was constructed to address the information needs of the project, with questions intended to solicit the key information required for the project. When in-person (physically or by phone) interviews could not be arranged, due to language facility or time commitments, the interview guide was provided to the participating DPA to be completed as a questionnaire. A copy of the interview guide is included in this report as an annex (Annex 1). Where circumstances allowed and participants were willing, the interviews were recorded and transcribed. Where this was not possible, the interviewer took notes. Some participants requested the opportunity to reply to the questions in written form, and this was provided when requested. Annex 2 of this Deliverable lists the DPAs interviewed by the PHAEDRA II consortium partners, as well as details about the specific interviewees. The consortium interviewed 27 representatives, covering nearly all Member State national DPAs, one German state DPA (*Landesbeauftragter für Datenschutz*) representative (In addition to the Federal DPA and because of the particular data protection context in Germany). Interview participants as well as Advisory Board were provided with a pre-publication draft of the report and invited to suggest corrections, clarifications and to make comments.

The interview research process takes participants perspectives as valid perspectives, which can feed into a larger discussion. This means that even where there is potentially disagreement about factual

[1] In this report, the first project is designated as PHAEDRA, the current stage as PHAEDRA II.

issues, these perspectives are meaningful for the DPAs involved. This document offers the potential for bringing some of these issues to the surface. 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 per cent), where as "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.

2 Main developments of the General Data Protection Regulation and their impact on co-operation between European DPAs

2.1 Introduction

The proposed GDPR will make co-operation between European DPAs a requirement. 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). 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". We asked participants what impact they envisaged that the passing of the GDPR, and particularly those provisions directly related to co-operation, would have upon their ability to co-operate and co-ordinate with other European DPAs.

Most DPAs anticipated a significant, strong impact from the passing of the GDPR in general, and particularly for co-operation between European DPAs. The stance of many DPAs towards the GDPR was optimistic, although this was often balanced with some caution, or recognition of additional work that needed (and needs) 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 that were highly sceptical about the GDPR. Participants reminded us that co-operation between European DPAs was already on-going 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 interviewed recognised the need for increased collaboration within the European Union. Several DPAs informed us that they expected the drive to more frequent co-operation would come primarily from both European citizens and business, who would, under the GDPR, have increased expectations about co-operation and consistency from their interactions with European DPAs, and that this would increase the onus upon DPAs to cooperate. DPAs expected the number of foreign 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. This differs from our assumption under PHAEDRA II that resource issues and the desire to avoid duplication of effort in enforcement would be primary drivers for co-operation and co-ordination. 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 co-operation would become increasingly routine, and part of the "daily life" of EU DPAs. Others DPAs suggested that increased co-operation would, over time, smooth out and routinise interactions between DPAs, and building upon successful examples and interactions would help to create a culture of co-operation which could improve over time. Additionally, it was suggested that potentially, the obligation to cooperate under the GDPR could provide additional weight to requests for co-operation. In general, DPAs believed

that increased co-operation 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 co-operation 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 co-operation. The need to find a systematic solution to the issue of multiple working languages was raised by several DPAs (in relation to several of our discussion topics). DPAs pointed out that the GDPR would not regulate all forms of co-operation. A number of DPAs offered information on the measures they were taking to prepare for the passing of the GDPR, including actions they would be having 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.

2.2 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".[2] 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 assistance to be reported to the EDPB, 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 way that citizens would encounter or interact with the mechanism and the time limits for decisions.

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

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 loosing 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).

2.3 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 EU.[3] 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 protection rights by European citizens, and towards facilitating 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 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 on-going discussions and dialogue, and some stated that more recent versions of the

[3] Article 51 (of the Commission version) "Where processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor will be competent for the supervision of the processing activities of the controller or processor in all Member States without prejudice to the provisions of Chapter VII of this Regulation". European Commission, *Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 Final, Brussels, 25.1.2012, http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM%282012%290011_EN.pdf. The Parliament version amends this to "Each supervisory authority shall be competent to perform the duties and to exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State, without prejudice to Articles 73 and 74. Data processing by a public authority shall be supervised only by the supervisory authority of that Member State". http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212

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.

2.4 The European Data Protection Board

The GDPR envisages the formation the European Data Protection Board (EDPB), a body composed of the heads of the supervisory authorities of each Member State and the EDPS, which would replace the Article 29 Working Party.[4] We asked DPAs for their perspective upon the proposed European Data Protection Board, the implications for co-operation between European DPAs and the impact of the shift from the 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 on-going.

A general perspective was that the EDPB would be a positive development. Co-operation 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.

Co-ordination, 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. DPAs from a country with a federal system for instance, raised the issue of

[4] see Articles 64-72 of the Commission draft, European Commission, 2012, *op. cit.*

how to determine their voting rights within the EDPB, an issue which is currently in discussion amongst the affected parties.

2.5 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[5] discussion process between the Commission, Council and Parliament before the GDPR could be finalised.[6] Several DPAs deferred on this question, citing a division (either explicitly constitutional/legal or conventional) between law-making and enforcement roles, which placed the negotiation process in the hands of Member State representatives. For example, one DPA told us that their foundational legislation, placed responsibility for data protection policy in the hands of Ministry of Justice. 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. 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.

[5] 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.

[6] There were a small number of responses to this question (5) as it was a question that was dropped from some interviews because of time constraints and prioritisation of other lines of questioning.

3 Challenges to co-operation between European DPAs

3.1 Sharing information

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 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 of 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, DPA 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 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). 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 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 meaning that European DPAs would start acting as, in a certain sense, a "big, single DPA" (consistency mechanism and one-stop shop, and an EDPB with binding decisions)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.

3.2 Structured systems for information exchange

We asked DPAs if they would value a structured system for the exchange of information with other DPAs. If so, we asked what safeguards would be required for such a system and what types of information would they be most interested to share? In our interviews we initially left the concept of a "structured system", and what this would mean, open, but provided some potential examples if asked.[7]

3.2.1 General remarks

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 a large number of 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.

[7] Including templates for particular types of communication, an Internet based communication system or network, particular communications tool, or some form of shared database.

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 co-operation and co-ordination. Clever and well designed systems for information exchange would likely not harm DPA co-operation, 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 co-ordination between DPAs, the issue of language was raised in this context: which language(s) would a structured information exchange system support? Active and on-going translation would be an expensive cost.

DPAs suggested that a 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.

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.

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 on-going investigations, potentially based upon that developed by the Belgian DPA for the *Google Spain* judgement[8];
- 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;
- 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 Communication and Information Resource Centre for Administrations, Businesses and Citizens (CIRCABC)[9], an existing communications tool. One DPA felt that the tool was a good one, but that it was current under-used. Others expressed doubts,

[8] Judgment of the Court (Grand Chamber) of 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/liste.jsf?num=C-131/12

[9] CIRCABC is a tool for the distribution and management of documents across mutliple langauges 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

particularly that they tool was not designed for this purpose, was not controlled nor owned by DPAs, and was not integrated with the day-to-day workflows of any authorities.

3.2.2 Safeguards

Safeguards for an information exchange system suggested or required by DPAs included standard technical and organisational measures, encryption, user authentication and control/access limitation, that the system was limited to authorized employees of European DPAs (and perhaps to employees in particular roles), administrative control of the system by DPAs, and higher standards and measures if personal data was to be exchanged on the system.

3.2.3 Barriers

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.

One DPA shared their experience of another DPA refusing to share information on an investigation of a multinational corporation. In this case, according to the interviewee, another DPA had refused to share details of a complaint, how it intended to investigate and the outcome of the investigation. The result being that co-operation was hard to achieve in this context.

3.3 Sharing best practice

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,[10] 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.)

[10] 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

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 Co-ordination and co-operation regarding enforcement

4.1 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 co-operation and co-ordination. 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 co-operation 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 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 co-operation 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 co-operation. One DPA expressed concern that a standardised approach might actively hinder and limit co-operation 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.[11] DPAs provided examples of systems in different fields that could be used as examples and inspiration for data protection.

[11] 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

These included the field of asylum claims, the system for passing on fines for violations of traffic rules between different EU states, criminal law co-operation 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.

4.2 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 co-ordination should be a DPA "leadership role".

The majority of DPAs interviewed suggested that the authorities themselves should play the leading role in co-operation and co-ordination between data protection authorities, in order to maintain their independence and effectiveness. DPAs were also seen as the site of knowledge and experience on co-operation and on enforcement. This extended to the development of specific frameworks and methodologies for co-operation between them. Co-ordination 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 co-operation framework they would use.

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 in some contexts 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 co-operation and co-ordination 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 co-operation or work of DPAs.

In discussing leadership roles more broadly, DPAs raised the issue of "lead DPA" in investigations,[12] and the way in which the EDPB could play a role in determining lead DPA and main establishment when there were disagreements.

4.3 Alerting tools

DPAs were asked if the GPEN alerting tool[13] 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 co-operation, 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.

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 co-operation. 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.

---

[12] The concept of the "Lead DPA" envisaged in the GDPR.

[13] Global Privacy Enforcement Network. For an outline of GPEN's composition and activity, please see PHAEDRA project report *Co-ordinationand Co-operation 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

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

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 forums 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 (e.g. mutual assistance, the consistency mechanism, one-stop-shop and join 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.

4.4 Budget for cross-border investigations

DPAs were asked if their participation in an investigation was requested 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, i.e. a 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 co-operation 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 co-ordination in this respect, they expected properly organised cross-border co-operation 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 (cf. Recital 94 and Article 47) that Member States should provide national DPAs with the resources necessary for co-operation, 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. This might allow larger and better resourced DPAs to support their smaller partners in investigations. Also mentioned was 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 co-operation 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.

4.5 Public communication in joint enforcement activities

DPAs were asked how they coordinated communication with the public (e.g. press releases or public reports) during or as part of the results of joint enforcement activities.[14] Several DPAs told us that they did not have any experience of specific communication co-ordination in this respect. Either they had not participated in what they considered joint investigation activities, or if they had, they had not coordinated their public communication. The common experience in this was that DPAs were primarily engaged in public communication with the population in their own jurisdiction, and on the findings of their own investigation (if these are routinely published).

Some DPAs did perceive a need to agree with other DPAs how to communicate any joint enforcement activity to the general public, as part of more generally improving communication practices, but that this remained open. Different DPAs currently have different communication

[14] This question was omitted from some interviews due to time constraints.

practices (some did not publish their enforcement activity until it was concluded, whilst others published some information during the process).

Article 29 Working Party has issued press releases as the coordinating body for European DPAs. The Nordic DPAs have issued joint press releases in some contexts, but have also issued individual national press releases in other contexts of co-operation.

5 DPA opinions and perspectives on PHAEDRA II activities

One of the intentions of this interview exercise was to consult with DPAs regarding their perspectives on some activities proposed as part of the further PHAEDRA II research project. These activities are intended to aid and support European DPAs in their co-operation and co-ordination activities. It is therefore important to understand if they are desirable for DPAs, if DPAs consider the activities to be worthwhile and useful, and to gain their perspective on the feasibility of the proposed activities as well as learn from them anything that should be taken into account in the pursuit of these.

We asked DPAs for their opinion on four activities:

- a repository collecting together key decisions by various DPAs,
- scoping and support for the development of a common approach to complaint handling,
- mapping the enforcement powers of European DPAs,
- looking at the potential activities of a technology watch function.

These efforts may enhance co-operation by bringing together existing opinions, allowing mutual learning, harmonisation, sharing experience, increasing the self-knowledge of the community of European DPAs and providing shared knowledge about potential future developments. The findings from these sections will be used to inform the on-going activities of the PHAEDRA II project.

5.1 Repository of decisions

DPAs were told that the project seeks to set up a repository of key decisions by EU DPAs, in order to make these easily and centrally available to other DPAs. They were asked if such a repository would be useful to their office.

Many DPAs were supportive of this activity. Having key decisions centrally and easily available (as well as searchable) was seen as an advantage. Even with a good DPA website, such materials could be difficult to find. One advantage of such a database is as a resource for staff through the DPA. We were told that, in the experience of one DPA, approximately 80% of cases they dealt with were broadly similar to cases they had already experienced; a good case-handling system was an important part of making the most of this existing learning. Similarly, another DPA said that the ability to refer people with questions to content already on their website was an advantage. Many DPAs expressed on-going interest in the decisions and findings of other European DPAs. These were seen as a source of learning and experience, and a source of guidance on issues and technologies etc., that the reader had not experienced, but that other DPAs had. DPAs stressed that learning from others' opinions avoided duplicating effort. This was particularly the case for smaller or newer DPAs. DPAs also identified that the existence of a central repository of decisions could be useful for citizens and data controllers.

Currently, DPAs use a number of methods to find out the decisions of their peers, with Google searches, accessing the DPAs individual websites, and emailed requests for information, being among the most common methods. Many DPAs informed us that they already published their key decisions, either as part of publishing all decisions, or through selecting particularly important ones. Several stated that their decisions were published on their website in relatively standard formats,

which might support automated archiving (HTML and/or PDF). Further DPAs suggested that they were beginning to publish summaries of key decisions online.

By far the most common issue raised in relation to a repository was that of language and the question of translation. Several DPAs suggested that the decisions in the repository would need to be translated into "an understandable" or a "commonly used" language. Some bi- or multi-lingual countries already publish decisions in more than one language. Others translate decisions that they believe will have an international impact (and in this cases, the translation tends to be into English). Even if a common set of languages could be agreed upon (English being a strong candidate), it would have to be determined who would carry the cost for translation purposes – the DPA publishing the decision, a responsible body or agency, or a third party. One suggestion was the mutuality scheme used by the Association of Francophone Data Protection Authorities (*Association Francophone des Autorités de Protection des Données Personnelles, AFAPDP*). The Association has a budget for translation costs to which DPAs contribute in proportion to their budget and their number of inhabitants. This funding model has been used by the Association to pay for translation of material for the Spring- and International Conferences.

A second issue was the risk of asking DPAs to contribute material (such as opinions) to too many co-ordination and aggregation platforms, particularly given existing resource demands upon DPAs. Therefore there was a risk of the PHAEDRA II project duplicating existing effort *and* asking DPAs to do so. There is apparently an initiative under the Spring Conference for creating a database of DPA decisions and our attention was directed towards the WorldLII International Privacy Law Library,[15] which has already started to host decisions by data protection authorities, and does so by archiving web-content with no overheads for the DPAs. There appears to be possibility to align PHAEDRA's activity with that of the Library.

Other requirements included clear rules and agreed formats for decisions. If the intention was to share key decisions, then some criteria for what constituted the key or most important decisions would need to be established and agreed. Some DPAs identified that they already had a procedure by which they identified what they considered their key decisions (For example, cases that are widely applicable, decisions that are often the subject of questions from the public, or significant enforcement actions. Rules would also have to be agreed on if (and how) decisions should be identifiable or anonymised (depending upon the public accessibility or not of the repository).

The interviews followed up the questions about the usefulness of such a repository with a direct question regarding if the DPAs would be willing and able to contribute to such a repository. No DPAs stated that they would be unwilling or unable to contribute to such a repository (given the issues raised above), a minor felt they were in a position to contribute to such a repository in full immediately (mainly because they were already publishing all their decisions, with some automation, and in either a very commonly used language or languages. The majority of DPAs felt able to contribute to such a repository if certain challenges and barriers were addressed properly. Some of these were internal issues (e.g. the human resources needed to contribute) and others were external (e.g. need to reach agreement on rules).

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

5.2 A common approach to complaint handling

We asked the DPAs if they would support the development of a common EU approach to complaint handling and if they considered such an approach to be desirable and feasible.

Several DPAs expressed support therefor, 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 producing a drive 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 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. This DPA advocated for this work with the PHAEDRA II project, adopting a comparative and critical perspective on the way that DPAs currently conduct complaint handling, the problems that might emerge from the GDPR and how these could be handled.

Some DPAs did speak about their own approach to complaint handling in the interviews, and some of the strategic and practical concerns that shaped it. A common approach to complaint handling might restrict some of the flexibility in this area, and might lead to two levels of complaint handling at European and then in national-level cases.

5.3 Mapping enforcement powers

One activity of the PHAEDRA II project is the mapping of the enforcement powers of DPAs. We asked DPAs if they felt this would be a useful exercise, and if they could make use of a centralised database of the foundation legislation granting DPAs their authority and powers, or if a mapping exercise would need to summarise powers and capacities more succinctly.

Several DPAs expressed their support for the activity. This was based upon the advantages of knowing the capacities of other DPAs when it came to joint investigations and other forms of co-operation, such as sharing information. Knowing what others were capable of, without having to ask direct questions was seen as potentially aiding planning activities, particularly in their initial early stages. It was also seen as potentially useful when a complaint from a data subject has to be channelled through another country. DPAs acknowledged the often significant differences between their capacities and their enforcement powers under the current framework. Differences raised included access to police files, sanctions and the ability to levy fines (of differing amounts). Having powers visible was seen as relatively important goal.

DPAs generally did not think that a straightforward gathering of foundational legislation would be sufficient or particularly useful, given that such legislation could exist across and make reference to multiple acts, and a reader would have to be able to parse these potentially complex legal documents in order to understand the particular powers of a fellow DPA.[16] Therefore a mapping exercise would need to extract competencies from the foundational legislation, and make the former available in a more structured, easily understood, comparable form - some form of "country fact sheet". Other information on this could include international contact points for key issues. Mapping the enforcement powers of the EDPB was also raised in this context.

Some DPAs did not see any added value from the creation of such a map or database. In this case they either felt familiar with the enforcement powers of their peers, or did not believe additional information would alter their decision making. Several DPAs informed us that they felt that this activity had been performed previously and that the results of these exercises should be available. The Article 29 Working Party, the European Commission and other parties may have performed mapping exercises. DPAs felt that they had certainly answered similar questions in the past.

A fundamental issue raised by DPAs in this context was the extent to which this exercise would be conducted before the passing of the GDPR, or afterwards. As a Regulation, some DPAs felt that the GDPR would harmonise the enforcement powers of DPAs. They therefore saw little value in conducting a mapping exercise that would be accurate for only a small number of months, until the Regulation is passed. A mapping exercise conducted afterwards would, theoretically, reveal little difference between the enforcement powers of European DPAs. A more nuanced approach for the mapping exercise was therefore seen as necessary by some DPAs – the mapping exercise would not focus upon core enforcement powers under the GDPR, but instead upon the way that the enforcement powers in the GDPR interacted with additional and existing legislation at the Member State level (for example administrative law, audit laws, laws on minor offenses, etc.). One DPA raised

[16] For examples of such mapping exercises on data protection laws, see: http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf and http://dlapiperdataprotection.com/#handbook/about-section/c1_BE

the challenge that a mapping of DPA enforcement powers might, to be meaningful, also have to map DPA enforcement strategies (for example, the balance between education, consultancy and enforcement, and the willingness to use particular powers) and that this would be a political issue for DPAs. However, in the post-GDPR context, a global mapping exercise was still seen as useful.

5.4 Technology watch.

A final activity of the PHAEDRA II project is looking into the potential for "technology watch" – the extent to which DPAs engage in technology foresight activities, either individually or as a collective community. We asked the interviewees if their authorities conducted analyses of emerging technologies for potential privacy and data protection issues. We also asked if they did do this, if the results were shared with other DPAs. We followed up by asking for their opinions and perspectives upon the value of a technology watch "taskforce" to collectively engage in this activity.

Many DPAs, particular smaller authorities, told us that they did not have the resources to conduct such activity in a systematic way, or to dedicate particular members of staff to this task. This did not mean that they did not have an interest in developing technologies, but that this was often done on an *ad hoc* or case-by-case basis by staff with other roles. Some DPAs felt that their learning about new technologies was somewhat driven by the complaints they received, the cases that they investigated, and external queries (e.g. from journalists). These smaller DPAs were interested in the technology watch activities of their larger peers, who have technology specialists, and see value in learning from these. Information on technology trends and potential future risks is exchanged by DPAs through working parties, joint events, and the personal networks of technology specialists. Some DPAs had specific expertise in this area, and provided information on their technology watch methodologies, including the way that they drew in information from external bodies. Across the DPAs interviewed there was a strong sense that keeping on top of technological developments (including drones, domestic CCTV, Internet of Things, big data, algorithm transparency, intelligence analytics and wearable computing) was a very important task. A related use for such a task force might also be to contribute support to forensic IT investigations where smaller DPAs lack the capacity for this.

Collecting together technology experts from European DPAs into a technology watch taskforce, with the capability to better share expertise, seemed to have some support from DPAs as this activity is currently somewhat dispersed. Many DPAs pointed out the existence of the Article 29 Working Party Technology Sub-Group as an area where this activity was already taking place (including recently on the Internet of Things, wearable devices and cloud computing[17]). The transition to the EDPB might recompose this group. However some DPAs suggested that the activity of the Technology Sub-Group was primarily driven by responding to issues raised by the plenary meeting of the Working Party, and that this did not leave too much capacity for horizon scanning. Additionally, the International Working Group on Data Protection in Telecommunication ("Berlin Group")[18] was identified as another group that already engaged in some technology-watch activities and was a good forum for

[17] Article 29 Data Protection Working Party, *Work Programme 2014-2015*, 3 December 2013, Brussels, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp210_en.pdf

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

information exchange. The capacity to contribute personnel and the demands of such a task force would still have to be agreed.

Whilst one DPA linked technology watch to encouraging technology companies to perform more Privacy Impact Assessments (PIAs), another DPA issued a caution that a technology watch task force should be staffed by DPA personnel in order to ensure that it was not overly influenced by major technology companies. As a consequence, an independent site of technological expertise was seen as important.

6 General conclusions

The aim of these interviews was to support the PHAEDRA II project's goals of identifying, developing and recommending measures to support practical co-operation between European DPAs, and in particular to identify the challenges for cooperation arising from the reform of the European data protection framework. The interviews have been able to draw out the perspectives of European DPAs, the challenges faced by DPAs in this period, as well as some of the needs that DPAs have.

Most DPAs anticipated a significant**, strong impact from the passing of the GDPR** in general, and particularly for co-operation 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 co-operation 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 EU (which was seen by some as critical, given that a spirit or attitude of co-operation may be as important as specific legal provisions for co-operation). Several DPAs informed us that they anticipated the GDPR reforms to act as driver for more frequent co-operation. This differs from our assumption under PHAEDRA II that resource issues and the desire to avoid duplication of effort in enforcement would be primary drivers for co-operation and co-ordination.

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 co-operation required by the GDPR, particularly through the consistency mechanism, one-stop-shop and the EDPB 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 co-operation and co-ordination between European DPAs. For a minority of DPAs, the creation of structured systems for information exchange, shared complaint handling strategies, templates, forms, alerting systems, etc. were likely to be necessary given the scale of co-operation 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 co-ordination 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 remains a key topic of discussion in these interviews. **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.[19] Further research might understand the real extent of this problem in practice, and the number of languages required for effective co-operation.

Tools – including communication, information exchange, alerting tools and systems for structuring requests – were seen as generally useful, but not the limiting factor for co-operation. There are some existing tools (and phone calls, emails, and face-to-face meetings should not be discounted in DPA co-operation) 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 organisation, DPAs have staff turnover, and experience and knowledge distributed amongst a peer group can potentially be lost, either permanently or temporarily disconnected from that network by changes in personnel. 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 a 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

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

working out of these cooperative relationships, and the development of further institutionalised measures in response.

Annex 1 – PHAEDRA II interview guide

GDPR

1. The proposed data protection regulation will make co-operation between European DPAs a requirement. What impact do you envisage the passing of the GDPR will have upon your ability to cooperate and co-ordinate with other DPAs?
2. Which provisions/aspects of the new Regulation will be the most helpful for improving co-operation and co-ordination between data protection authorities?
3. What is your view on currently developed version of provisions on consistency mechanism/obligation to consult (article 57), One-stop-shop and the role of the European Data Protection Board? Which issues should be raised by DPAs before the Trialogue starts?

CHALLENGES

I. Sharing information

4. The proposed regulation (GDPR) would require DPAs to share "relevant" information with each other. How would you determine "relevant"?
5. Would you value a structured system for the exchange of information with other DPAs? What safeguards would be required? What types of information would be the most interested to share?
6. Are there any barriers to your use of such as system?
7. How do you currently share information on best practice with other DPAs?

II. Co-ordination and co-operation regarding enforcement

8. Would a standardised EU approach to "requests for assistance" be useful?
9. What role (if any) would you like to see the European Commission take in the development of a co-operation framework for DPAs? Should this be a DPA "leadership role"?
10. Would the GPEN alerting tool be sufficient for you or would you 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?
11. If you were asked to participate in an investigation by another EU DPA, would you have budget for this? In joint enforcement activities, how are public communications coordinated?

III. Privacy risk assessment

12. Do you have a structured process for assessing privacy risks?

PHAEDRA II ACTIVITIES

I. Repository

13. The project seeks to set up a repository of key decisions by EU DPAs, in order to make these easily and centrally available to other DPAs. Would such a repository be useful to your office?
14. Would you be able to contribute material to such a repository? Do you see any obstacles for that contribution (e.g. the relevant language used)?

II. A common approach to complaint handling

15. Would you support the development of a common EU approach to complaint handling? Would this be desirable or feasible?

III. Mapping enforcement powers

16. One activity of the PHAEDRA II project is the mapping of the enforcement powers of DPAs. Would it be useful do it and to have access to a centralised database of the foundation legislation granting DPAs their authority and powers?

V. Technology watch

17. Do you conduct analyses of emerging technologies for potential privacy and data protection issues? If so, are these shared with other DPAs?
18. Do you see any value in a technology watch "taskforce"?

Annex 2 – Participating Data Protection Authorities

DPA
Comissão Nacional de Protecção de Dados (Portugal)
Commission Nationale de l'Informatique et des Libertés (France)
Garante per la protezione dei dati personali (Italy)
Agencia de Protección de Datos (Spain)
Österreichische Datenschutzbehörde (Austria)
Datainspektionen (Sweden)
Information Commissioner's Office (United Kingdom)
Office of Data Protection (Finland)
Federal Commissioner for Data Protection and Freedom of Information, Berlin
Croatian Personal Data Protection Agency
National Authority for Data Protection and Freedom of Information (Hungary)
National Supervisory Authority for Personal Data Processing in Romania
State Data Protection Inspectorate of the Republic of Lithuania
The Office for Personal Data Protection of the Slovak Republic
Information Commissioner (Slovenia)
Commission de la protection de la vie privée (Belgium)
Commission for Personal Data Protection (Bulgaria)
Commissioner for Personal Data Protection (Cyprus)
The Office for Personal Data Protection (Czech Republic)
Estonian Data Protection Inspectorate
Der Bundesbeauftragtefür den Datenschutz und die Informationsfreiheit (Germany)
Data Protection Commissioner (Ireland)

Datu ValstsInspekcija (Latvia)
Commission nationale pour la protection des données (Luxembourg)
Office of the Data Protection Commissioner (Malta)
Dutch Data Protection Authority (Netherlands)
Generalny Inspektor Ochrony Danych Osobowych (Poland)
European Data Protection Supervisor