PHAEDRA

Improving **P**ractical and **H**elpful cooper**A**tion betwe**E**n **D**ata P**R**otection **A**uthorities

http://www.phaedra-project.eu/

CALL: JUST/2011-2012/FRC/AG
AGREEMENT NUMBER: JUST/2012/FRAC/AG/2761

Workstream 4: Findings and recommendations

Deliverable 4: Findings and recommendations

Prepared for the European Commission
Directorate General Justice
Co-funding by the Fundamental Rights & Citizenship Programme

Brussels, January 2015

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

Contributors	
Name	**Partner**
Artemi Rallo	Jaume I University
Paul de Hert	VUB-LSTS
Gertjan Boulet	VUB-LSTS
Dariusz Kloza	VUB-LSTS

Internal reviewers	
Name	**Partner**
Artemi Rallo	Jaume I University
Rosario García Mahamut	Jaume I University
Paul de Hert	VUB-LSTS
Gertjan Boulet	VUB-LSTS
Dariusz Kloza	VUB-LSTS
Antonella Galetta	VUB-LSTS
Beata Batorowicz	GIODO

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

Contents

1 Introduction

This report synthesises the key findings and recommendations from the PHAEDRA project's D1, D2.1 and D2.2 deliverables. It also contains some new information: it summarises the results of the PHAEDRA workshops and conferences.[1] It provides the results of the second and third PHAEDRA surveys; and it provides the collective recommendations of the PHAEDRA consortium.

A principal challenge confronting data protection authorities (DPAs), privacy commissioners (PCs) and privacy enforcement agencies (PEAs) is the enforcement of privacy and data protection legislation. As privacy and personal data breaches (torts, contraventions and crimes), due to recent technological developments, often do not stop at the frontiers of a single jurisdiction, there is a critical need for an effective and efficient cross-border co-operation of relevant authorities, especially since there are fundamental rights at stake. DPAs face constraints by way of human and/or budgetary shortages, institutional and legislative rules and other factors, to investigate and prosecute those who violate the law.[2] Often, these resource-constrained DPAs may also investigate the same privacy issue, in effect, a duplication of effort. Given the constraints of most DPAs, it seems an inefficient use of resource to have several DPAs investigating the same issue.

Because of these problems, and other barriers to co-operation and co-ordination,[3] stronger and more enhanced cooperation among DPAs is not only desirable but also necessary. DPAs themselves have recognised the need to improve practical co-operation, and the EU Data Protection Reform is also going in this direction. Articles 45 and 55 of the European Commission's proposal for a new Data Protection Regulation (2012) explicitly provide for regional and international co-operation mechanisms, respectively.[4] Thus, the crucial issue here, better co-operation and co-ordination between DPAs should be introduced, better explained and more emphasised.

PHAEDRA, a two-year project that began in January 2013, is co-funded by the European Union under its Fundamental Rights and Citizenship Programme, and is aimed at adding value, complementing and supporting the initiatives of DPAs to improve international co-operation and co-ordination among them. PHAEDRA thus builds upon recent efforts to improve co-operation and co-ordination in the enforcement of privacy laws.[5] The project has gathered and analysed information on the matter and has interacted with DPAs via interviews, surveys and workshops in its efforts to advise on the improvement of practical co-operation and co-ordination. The PHAEDRA consortium conducted case studies of where two or more DPAs have investigated the same privacy issue and other case studies where DPAs collaborated. It identified and evaluated existing mechanisms for co-operation between DPAs.

[1] See also, PHAEDRA, "Executive summary of Deliverables 3.1 and 3.2: Contact list of Data Protection Authorities (DPAs) and collaboration with GPEN and the ICDPPC working group", Brussels, January 2015. http://www.phaedra-project.eu/?page_id=201; Deliverable 3.4, "PHAEDRA workshops and final conference", Brussels, January 2015. http://www.phaedra-project.eu/?page_id=201

[2] One DPA commented to the authors that "There is a solid amount of non-used resources and opportunities to improve the international and domestic work of DPAs."

[3] See below, section 7 on barriers.

[4] See below, section 3.2 on mechanisms for co-operation at the European level.

[5] See below, section 3 for an overview of networks of co-operation between DPAs.

It identified different forms of co-operation and co-ordination between DPAs, and other areas beyond enforcement where co-operation could offer practical benefits to all concerned.[6]

The PHAEDRA consortium also reviewed the legislation establishing DPAs to identify whether there are provisions that facilitate or act as barriers to international co-operation and co-ordination, and what measures could be taken to reduce such barriers. The PHAEDRA consortium also held four workshops for DPAs, and searched for collaboration with the Global Privacy Enforcement Network (GPEN) and the International Conference of Data Protection and Privacy Commissioners (ICDPPC).[7] As the issue of co-operation and co-ordination is not exclusive to the area of data protection, the PHAEDRA consortium also comparatively analysed the enforcement mechanisms in international and European competition law.[8] Finally, given the theoretical possibility for DPAs to tackle privacy conflicts with a criminal law dimension via mutual legal assistance treaties (MLATs), some criminal law instruments were discussed as an illustration.

2 Case studies

2.1 Case studies in the European Union

The case studies focused on instances of where two or more DPAs investigated the same issue (e.g., Google Buzz and Google Street View vehicles gathering WiFi addresses, Facebook's collection of personal data for sale to third party apps developers and advertisers, the hacking of Sony PlayStation). The case studies focused not only on how improved co-operation would have been beneficial if it had occurred, but also on instances where there was co-operation. The case studies highlighted the success of the Art. 29 WP as a model of co-operation between DPAs, at least, in regard to some issues.

Here is a thumbnail sketch of some of the cases PHAEDRA examined. There have been instances where DPAs undertook their own individual investigations (e.g., Google Street View) and other instances where two or more DPAs collaborated (e.g., Google Buzz, Google's privacy policy, WhatsApp).[9]. In the Street View case, there was arguably a huge duplication of effort, the lessons of which were not lost on DPAs who improved their co-ordination in subsequent investigations.

From the Google Street View case, PHAEDRA found that

- There was no global system of co-ordination among DPAs that enables them to co-ordinate investigations in different countries of identical privacy breaches. Article 28.6 of Directive 95/46/EC calls for co-operation between DPAs, but there are different interpretations of the legal basis in different countries' domestic laws on how far it allows a DPA to share information in the specific context of enforcement cases. In any case, the Directive only applies to the EU, not globally.

[6] See below, section 8.2 on aims and forms of co-operation.
[7] See below, section 3 on networks,
[8] Cf. Kloza, Dariusz, and Anna Moscibroda, "Making the case for enhanced enforcement co-operation between data protection authorities: insights from competition law", *International Data Privacy Law*, Vol. 4, No. 2, 2014, pp. 120-138. http://idpl.oxfordjournals.org/content/4/2/120.full.pdf+html; Kloza Dariusz, Anna Moscibroda and Gertjan Boulet, "Improving Co-operation Between Data Protection Authorities: First Lessons from Competition Law", *Jusletter IT. Die Zeitschrift für IT und Recht*, Weblaw AG, Issue 20,2013. http://jusletter-it.weblaw.ch/magnoliaPublic/issues/2013/20-Februar-2013/2128.HTML
[9] Unlike Google in the case on Google's privacy policy, WhatsApp complied with the recommendations of the Canadian and Dutch DPAs.

- There was no global system that enables co-operation among DPAs for harmonising legal criteria and adopting identical resolutions on identical breaches of privacy. Even the current European system under the Data Protection Directive – which gives interpretation functions to the Art. 29 WP – did not avoid divergence among national DPAs.
- Limitations set forth in national laws (e.g., confidentiality provisions) make difficult or impossible an effective co-ordination of investigation procedures on identical breaches.
- Google benefitted from the absence of global co-ordination mechanisms to establish a single, direct and bilateral relationship with DPAs that generated confusion.

The Google Buzz case suggested that co-ordinated expressions of shared concern on the part of voluntary groups of DPAs are possible, but that these measures do not always involve all parties that may have concerns or the potential for enforcement processes. A collectively signed letter is a relatively minor form of co-operation, with potentially limited impact; however, it does show some agreement of key issues relating to a new service or technology.

In 2012, the Art. 29 WP mandated the 'Commission nationale de l'informatique et des libertés' (CNIL, French DPA), to investigate Google's new privacy policy. At the end of the investigation, the WP29 issued a set of recommendations to Google. In February 2013, following insufficient compliance by Google with the WP29's recommendations, the WP29 established a taskforce of six DPAs, led by CNIL, and comprising five other DPAs (Germany, Italy, Spain, UK and the Netherlands). Following unsuccessful meetings between Google and the task force, the members of the task force launched their own investigations on compliance of Google's privacy policy with national legislation, but as "part of an international administrative cooperation".[10] The CNIL and Spanish DPAs have already imposed fines on Google, and the Dutch DPA has threatened to do so. The chairman of the Dutch DPA, Jacob Kohnstamm, stated that "European DPAs had learned from previous investigations into Google Street View that a co-ordinated approach was more effective for looking at Google's privacy policy".[11] This is undoubtedly an example of best practice in improving co-ordination between DPAs.

In some instances (e.g., the Irish DPA's audit of Facebook Ireland), the DPA undertook the investigation but drew on support and/or findings from other DPAs. In other instances, DPAs have reached very different findings: in the instance of the Sony PlayStation case, to its credit, the Australian DPA informed other DPAs of its findings. In the SWIFT case, where SWIFT transferred Europeans' financial data to US authorities, there was broad agreement to delegate the initial investigation to the Belgian DPA, while the Art 29 Working Party acted as a point of co-ordination.

The Art 29 Working Party has co-ordinated other investigations too, such as how communications carriers were implementing the Data Retention Directive, as well as the first Joint Enforcement Action regarding the data protection practices of private health insurance companies and the World Anti-Doping Agency (WADA).

The case studies demonstrate a strong central role of the Art. 29 WP in European collaboration. The Working Party has also engaged in some co-operation (information sharing

[10] CNIL, "CNIL orders Google to comply with the French Data Protection Act, within three months", 20 June 2013. http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-comply-with-the-french-data-protection-act-within-three-months/

[11] Gardner, Stephen, "Dutch DPA Concludes That Google Is in Breach of Data Protection Act", *Bloomberg BNA*, 2 December 2013. http://www.bna.com/dutch-dpa-concludes-n17179880411/

and parallel investigations) outside Europe. Nevertheless, there have been calls for changes even to the Art. 29 WP, which has led to the Commission's plan in the proposed new Data Protection Regulation for the Art. 29 WP to be replaced by a European Data Protection Board.

2.2 Case studies beyond Europe

Beyond Europe, the Global Privacy Enforcement Network (GPEN) co-ordinated the investigations of website's privacy policies by 19 DPAs in the first annual "Privacy Sweep" in May 2013 and of mobile apps by 26 DPAs in the second Sweep in May 2014. This is a good example of effective co-ordination between DPAs. The Canadian Privacy Commissioner initiated the actions. Even more DPAs, 37 in total, collaborated in the issue of a joint letter to Google seeking responses to questions about Google Glass, the Internet-connected glasses. This was another example of effective co-ordination and an example of "strength in numbers". Here is yet another example: On 9 December 2014, DPAs from around the world sent a letter to the operators of seven app marketplaces (Apple, Google, Samsung, Microsoft, Nokia, BlackBerry and Amazon.com) urging mandatory links to privacy policies for apps that collect personal information.[12] The letter was sent by DPAs from Canada (OPC, Alberta, British Columbia), Australia, Germany (Baden-Württemberg and Bavaria), Belgium, Colombia, Estonia, Finland, France, Gibraltar, Hong Kong, Ireland, Israel, Italy, China (Macao), the Netherlands, New Zealand, Norway, South Korea and the UK. As said, a collectively signed letter shows some agreement between DPAs of key issues relating to a new service or technology.

2.3 (De-)centralised modes of co-ordination

Several of the case studies undertaken by PHAEDRA demonstrated a perceived need among DPAs for collaboration driven by international data protection incidents and uneven responses to these. Co-ordination has arisen in response to an international data protection and privacy environment typified by different national jurisdictions, legal frameworks and particular contexts, and to data protection issues that cross multiple jurisdictions. One of the most common reactive modes of co-ordination is the collective identification of the local DPA that has local jurisdiction over an issue and then delegating to the local DPA the investigation of the issue, and giving it a strong role in any collective response. A second common mode of co-ordination is decentralised information gathering combined with centralised reporting or sharing of that information. This appears an effective response to many multi-national issues (for example, national DPAs contacting national central banks for information in the SWIFT case). Problems potentially arise when individual DPAs do not have investigation or audit powers, or have weaker sanctions than other DPAs.[13] They may therefore not be able to carry their weight in a delegated, multi-national investigation.

3 Mechanisms for co-operation

3.1 Active modes of co-operation

There are various mechanisms that foster international collaboration between DPAs. There is also good evidence of and a clear desire for information sharing between DPAs, even on

[12] Office of the Privacy Commissioner of Canada, "Joint Open Letter to App Marketplaces", News, 9 December 2014. https://www.priv.gc.ca/media/nr-c/2014/let_141210_e.asp

[13] See below section 4, on powers of DPAs.

unrelated cases because DPAs generally appear interested in learning from the experiences of other DPAs. For this reason, they engage in informal ad-hoc consultation and "watching with interest", which can also be seen as unco-ordinated and non-confidential forms of enforcement co-operation.[14] Co-ordination appears to be easier and occur more smoothly in active modes, when co-ordination has been planned and agreed in advance of an action, rather than reactive, where DPAs attempt to co-ordinate in response to a complaint or an unanticipated issue.

As said in the introduction, PHAEDRA is aimed at adding value, complementing and supporting the initiatives of DPAs to improve international co-operation and co-ordination among them. The PHAEDRA partners identified and evaluated existing mechanisms for co-operation and co-ordination in enforcement, within Europe as well as internationally, including co-operation and co-ordination between the EU and third countries. The key mechanisms are referenced in the following paragraphs.

3.2 Mechanisms for co-operation at the European level

Co-operation between DPAs has been a frequent topic of discussion at recent Spring Conferences.[15] The Case-Handling Workshop is a sub-grouping of the Spring Conference each time organised by a different DPA to help promote the exchange of information on case studies and practical issues at the operational level ("staff level"), as well as increasing general contacts between employees. Another subgroup of the Spring Conference was the Working Party of Police and Justice (WPPJ), which monitored developments in the area of police and law enforcement with regard to the processing of personal data. Its role was subsequently taken over by the Art. 29 WP.

DPAs currently co-operate on the basis of Article 28(6) of Directive 95/46/EC, which requires DPAs to collaborate with each other. The proposal for a General Data Protection Regulation (GDPR) aims to strengthen collaboration between DPAs: it contains provisions on co-operation among the EU DPAs (Article 55 GDPR) and co-operation between EU DPAs and DPAs from third countries (Article 45 GDPR). Article 56 GDPR introduces rules on joint operations. Most innovative is the "one-stop-shop" principle introduced in Article 51 GDPR, which gives competence to the supervisory authority of the main establishment of the controller or processor for the supervision of the processing activities of the controller or the processor in all Member States.

Undoubtedly, the best example of co-operation and co-ordination between DPAs is the Art. 29 WP: The Art. 29 WP meets regularly, every two months or so, to discuss and come to agreement on various issues that affect many or all of its members. The Art. 29 WP has collaborated in the preparation of a large number of Opinions and issued joint letters to entities who are violating the provisions of the Art. 29 Working Party. No other network of DPAs has achieved so much. It was set up under Directive 95/46/EC and comprises representatives of the supervisory authorities of EU Member States, the supervisory authorities set up within the EU institutions and bodies, and a representative of the European Commission. The Opinions of the Working Party are not legally binding, and the Working

[14] See below, section 8.2 on forms and aims of co-operation between DPAs.

[15] Buttarelli, Giovanni, "How could DPAs better co-operate and provide leadership for the future", Spring Conference, Data Protection, Lisbon, 17 May 2013. http://springconference2013.cnpd.pt/wp-content/uploads/Giovanni-Buttarelli-Assistant-EDPS-%E2%80%93-How-could-DPAs-better-co-operate-and-provide-leadership-for-the-future.pdf

Party has no independent enforcement powers. The role of the Working Party is largely to advise the European Commission, but it has become a principal means of establishing both common views between European DPAs and more recently joint enforcement operations.[16] When the proposed GPDR comes into force, the Art. 29 WP will be superseded by the European Data Protection Board (EDPB).[17] The Art. 29 WP secretariat will pass from the EC to the European Data Protection Supervisor (EDPS).[18] The EDPB will have greater powers than the Art. 29 WP.[19] The focus of the Art. 29 WP has sometimes extended beyond Europe. For example, it established a co-operation with the Asia-Pacific Economic Co-operation to make the European Binding Corporate Rules (BCRs) interoperable with APEC's Cross Border Privacy Rules. In 2013, then Art. 29 WP chairman Jacob Kohnstamm was an observer at and addressed an APEC meeting in Auckland, the first time such an event has happened.

Another mechanism for co-operation at the European level is the Contact Network of Spam Authorities (CNSA) which comprises European anti-spam enforcement authorities. CNSA created a "Co-operation procedure concerning the transmission of complaint information and intelligence about spam", which aims at facilitating information sharing and joint investigation on cross-border spam cases. The co-operation procedure predated the 2014 'Global Cross Border Enforcement Cooperation Arrangement' adopted during the 2014 ICDPPC (see below, 8.4). Practical experiences of spam authorities in the implementation of the Cooperation Procedure may provide valuable lessons for implementation by DPAs of the Cooperation Arrangement.

The Council of Europe (CoE) Consultative Committee on the protection of personal data (the T-PD, which stands for *traité protection de données*) acts as a forum for exchanges on privacy challenges and developments. It was established under Chapter V of the CoE's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Chapter IV of Convention 108 includes extensive provisions on Mutual Assistance. Article 13 contains the general duty to render mutual assistance including the requirement to nominate at least one authority for these co-operative purposes. The primary duty is to provide information on law and administrative practice in the field of data protection. Article 14 requires the provision of assistance to foreign data subjects. Article 1(5) of the Additional Protocol to Convention 108 stipulates that "[i]n accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information". The Convention currently undergoes a modernisation aimed at, among others, strengthening co-operation among the authorities of its contracting parties.

3.3 Mechanisms in former EU-third pillar networks

DPAs have also co-operated in the context of the former third pillar supervision. The Schengen Convention abolished internal border controls and implements a common visa policy within Europe. The Schengen Information System (SIS) is a database that allows the participating states to share information for border control, national security and law enforcement purposes. In 2013, the second generation SIS replaced the previous system, providing enhanced functionalities, among others. This also resulted in a change how

[16] OECD, Report on the Cross-Border Enforcement of Privacy Laws, Paris, October 2006, p. 23.
[17] Preamble nr. 3.4.7.3 of the GDPR.
[18] Article 71 of the GDPR.
[19] Article 66 of the GDPR.

processing personal data therein is supervised: since 9 April 2013, it is the national DPAs and the EDPS. The previous Joint Supervisory Authority (JSA) ceased to exists.

The Customs Information System (CIS) was established under the 1995 Convention on the use of information technology for customs purposes and Council Regulation (EC) No515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and co-operation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters.[20] The aim of the CIS is to assist in combating customs-related crime by facilitating co-operation between European customs authorities. The CIS Convention divides the data protection of CIS between national DPAs and the Joint Supervisory Authority (JSA) for the Customs Information Service, which is an independent authority composed of two representatives of the DPAs of each Member State that signed this CIS convention.[21] The JSA performs its task in accordance with the provisions of the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes,[22] and of Convention 108 taking into account Recommendation R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe, regulating the use of personal data in the police sector.[23] The JSA for the Customs Information Service has a secretariat located in Brussels.

The European Visa Information System (VIS) is a database of information on visa applications from third country nationals. The Visa Information System Supervision Coordination Group comprises those DPAs with responsibilities for supervision of the VIS. Supervision of the central unit of VIS is the responsibility of the EDPS, whilst supervision of its operation and use at the national level is the responsibility of the respective Member State's DPAs.

EURODAC is a fingerprint database of applicants for asylum and illegal immigrants found within the EU. In order to ensure a co-ordinated approach between EPDS and the national DPAs in EU Member States that supervise the processing of data by national authorities and transmission to the central EURODAC unit, the authorities meet regularly as the EURODAC Supervision Coordination Group to discuss common problems, and seek common solutions.[24] The EURODAC Supervision Coordination Group is therefore a co-operation platform for the DPAs responsible for the supervision of EURODAC. The secretariat of the EURODAC Supervision Coordination Group is provided by and located at the EDPS in Brussels.

Europol was established in 1999 as an intelligence broker for co-ordinated police work in Europe. The Joint Supervisory Board (JSB) is Europol's independent data protection supervisor.[25] In the European Council Decision of 6 April 2009, Member States recognised the need to provide special, tailor-made data protection rules for Europol. Several entities monitor and ensure compliance with the data protection rules at Europol. These include the Data Protection Officer, the Joint Supervisory Body and National Supervisory Bodies. The

[20] Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and co-operation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, (EC) No515/97, OJ L 83, 13 March 1997, pp. 1-16.
[21] http://www.privacycommission.be/en/jsa-customs-information-system
[22] Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, OJ C 316, 27.11.1995, pp. 34-47.
[23] See Article 18.2 of the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes.
[24] EDPS, "EURODAC". https://secure.edps.europa.eu/EDPSWEB/edps/Home/Supervision/EURODAC
[25] Information on the activities of the JSB can be found at http://europoljsb.consilium.europa.eu/about.aspx

Joint Supervisory Body (JSB) is an independent entity set up to review the activities of Europol in order to ensure that the rights of the individual are safeguarded during the storage, processing and utilisation of personal data held by Europol. This body is composed of two representatives of the independent national DPA of each EU Member State, selected internally, who are appointed for a period of five years. The JSB is an accredited member of the Spring Conference and the International Conference of Data Protection and Privacy Commissioners.

Eurojust, the European Union's judicial co-operation unit, is responsible for encouraging and facilitating co-ordination of investigations and prosecutions between competent authorities in the Member States, making these more effective in dealing with cross-border crime. The Joint Supervisory Body (JSB) is an independent external supervisor of Eurojust in the area of data protection. The Eurojust JSB discusses compliance with the Eurojust data protection officer and can undertake spot inspections: it is entitled to have full access to all files where personal data is processed. Furthermore, "Eurojust shall provide the Joint Supervisory Body with all information from such files that it requests and shall assist that body in its tasks by every other means".[26] The JSB was accredited as an independent supervisory authority member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in 2010, and by the European Data Protection Commissioners' Conference in October 2011, and has a secretariat based in the Hague. Unlike the other EU JSBs discussed in this section, the Eurojust JSB is not necessarily composed of representatives of national DPAs (although several are members), but can also include judges and other similarly independent roles.

3.4 Mechanisms for co-operation at the global level

At the global level, there are various mechanisms that promote co-operation and co-ordination. Among them are the following:

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) has been meeting annually since its establishment in 1979. One of its objectives is to encourage and facilitate co-operation and the exchange of information among accredited members, in particular regarding enforcement actions. The Conference regularly issues resolutions. Decision-making in the closed session is based upon consensus when possible or by majority vote. Several of the International Conferences have adopted resolutions on international co-operation. The 29th Conference, held in Montreal in September 2007, adopted such a resolution. The 33rd Conference, held in Mexico City in November 2011, adopted a resolution on Privacy Enforcement Co-ordination at the International Level. [27]

The 35th Conference, convened in Warsaw in September 2013, issued a Resolution on International Enforcement Coordination.[28] The Conference resolved to bring about more effective co-ordination of cross-border investigation and enforcement, which shows clearly the growing importance of this issue for DPAs. The Conference mandated the International Enforcement Coordination Working Group (IECWG), established at the conference held in Mexico in 2011, to work with other networks to develop a common approach to cross border

[26] Article 23 the Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, 6 March 2002, pp. 1-13.
[27] The Resolution on Privacy Enforcement Co-ordination at the International Level is available here: http://privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_001_%20Intl_Priv_Enforc_ENG.pdf
[28] http://www.priv.gc.ca/information/conf2013/res_04_coordination_e.asp

enforcement and case handling expressed in a multilateral framework document. This aimed to build upon the work of GPEN and address sharing of information. The Resolution also encouraged DPAs to seek out opportunities to co-operate, and support the development of a secure information platform.[29]

The 36th Conference, held in Mauritius in September 2014, agreed a Resolution on Enforcement Co-operation and an agreement on Global Cross Border Enforcement Co-operation, the aim of which is to facilitate the sharing of information and enforcement co-ordination between DPAs.[30] The agreement, also known as an arrangement, offers various degrees of co-operation in recognition of differences in national legislation. The PHAEDRA consortium produced the first draft for the working group. The PHAEDRA consortium also commented extensively on the seventh draft. The agreement went through 16 drafts before it was finally adopted in Mauritius.

The International Working Group on Data Protection in Telecommunications (IWGDPT, also known as the Berlin Group) has been an important forum for co-operation since its creation in 1983 at the ICDPPC. The Group is composed of experts in communication and information technologies and in personal data protection. Its membership is not restricted to DPAs, and includes representatives from private sector and NGO organisations. The Group's work results in common positions and working papers on requirements and conditions that should be met both by products created by technology providers and by the entities using these products, e.g., telecommunications operators, web services and end-users of the products[31], in order to improve the protection of privacy.

The Organisation for Economic Co-operation and Development (OECD) has played an important role in promoting international co-operation and enforcement co-ordination. The OECD issued a Recommendation on 23 September 1980 that Member countries co-operate in the implementation of its Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.[32] In July 2013, the OECD produced a revision of its influential 1980 privacy guidelines.[33]

In October 2006, the OECD published a Report on the Cross-border Enforcement of Privacy Laws.[34] The report was based upon a questionnaire of OECD governments conducted by the Working Party on Information Security and Privacy (WPISP), now known as the OECD Working Party on Security and Privacy in the Digital Economy (SPDE).[35] The report recommended further consideration of several topics regarding co-operation, and provide an example of how co-operation among DPAs could be enhanced:

[29] The Resolution on International Enforcement Coordination is available here https://privacyconference2013.org/web/pageFiles/kcfinder/files/4.%20Enforcement%20coordination%20resolution%20EN%20.pdf

[30] The Resolution on Enforcement Co-operation and the Global Cross Border Enforcement Cooperation Arrangement; http://www.privacyconference2014.org/en/about-the-conference/resolutions.aspx

[31] GIODO, "Meeting of the Berlin Group, 23-24 April 2012". http://www.giodo.gov.pl/259/id_art/736/j/en/

[32] Organisation for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris, 23 Sept 1980. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[33] The revised guidelines can be found here: http://www.oecd.org/sti/ieconomy/privacy.htm

[34] OECD, *Report on the Cross-Border Enforcement of Privacy Laws*, Paris, October 2006, p. 26.

[35] OECD, "OECD Questionnaire on the cross-border enforcement of privacy laws", DSTI/ICCP/REG(2006)1, 2006. http://www.oecd.org/sti/ieconomy/37572050.pdf

- Examination of approaches to handling and classifying cross-border complaints.
- Work towards identifying common priorities for enforcement co-operation.
- Ways to improve co-operation between authorities with respect to notifications, information sharing, and investigative assistance.
- Consideration of the adequacy of sanctions and remedies available to privacy enforcement authorities in the context of cross-border cases.
- Work towards improving the enforcement of orders for monetary redress for individuals who suffer privacy breaches.
- Examination of informal methods of international co-operation – often through regional networks – that allow for information exchange on current issues and best practices.
- Consideration of the need for practical tools, such as contact lists, to request assistance from another authority, cross-border complaint forms, common approaches to reporting case results, etc.
- Work towards establishing a more complete and robust set of indicators about the dimensions of cross-border privacy problems.

Taking account of the Report, the OECD published a Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy in 2007.[36] The OECD recommended that member countries develop effective international mechanisms to facilitate cross-border privacy law enforcement. It recommended that they should provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.

Following on from the 2007 Recommendation, the OECD supported measures towards international co-operation between privacy enforcement authorities (PEAs). The OECD hosts the website and online platform for the Global Privacy Enforcement Network (GPEN).[37] Established in September 2010, GPEN aims to facilitate cross-border co-operation in the enforcement of privacy laws. Membership in GPEN enables privacy regulators from around the world to work more closely as they address risks to the personal information of their citizens. GPEN maintains a contact list of DPAs and operates an online platform for sharing information and providing different types of documents. As of December 2014, GPEN counted fifty PEAs, including DPAs and privacy commissioners (PCs). The GPEN website provides a restricted-access platform for sharing of documents and news. It also includes collaboration tools such as discussion forums, an events calendar and other functionalities. A few GPEN members, including the US, Canada and the UK, are developing and/or funding the development of an alert service. GPEN has developed an action plan which is available on its website. The GPEN action plan is not legally binding, and co-operation is subject to applicable laws in the jurisdictions involved.

3.5 Mechanisms for co-operation at the regional level

Another important regional forum for DPA co-operation is that provided by the Asia-Pacific Economic Co-operation (APEC), which includes representatives from 21 Pacific rim

[36] OECD, Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, Paris, 2006. http://www.oecd.org/sti/ieconomy/38770483.pdf
[37] www.privacyenforcement.net

countries who seek to promote free trade and economic co-operation throughout the region.[38] APEC published a Privacy Framework in 2005, which consists of nine principles to assist APEC countries in developing approaches to privacy that maximise privacy protection whilst at the same time encouraging the cross-border flow of information. The principles are preventing harm, notice, use, collection limitation, choice, security safeguards, integrity, access and correction, and accountability. The Framework also encourages member economies to develop co-operative arrangement and procedures to facilitate cross border collaboration in the enforcement of privacy laws, taking into account existing international arrangements and the requirements of domestic law.

APEC created a Cross-border Privacy Enforcement Arrangement (CPEA) as a framework for regional co-operation on privacy enforcement. The CPEA aims to facilitate information sharing between APEC privacy enforcement authorities, provide mechanisms for effective cross-border co-operation in the enforcement of privacy law, and to encourage information sharing and co-operation with privacy enforcement agencies outside of APEC. Participation in CPEA is required in order to also participate in the Cross-Border Privacy Rules (CBPR) system. CBPRs allow businesses to set out their practices for collecting and processing personal information, and to use these rules as internal procedures. The rules must comply with the APEC Privacy Framework and the national laws of the countries where the business operates.[39]

The EU and APEC established a Working Team in 2013 that aimed to develop interoperability between the European Binding Corporate Rules (BCRs) and the APEC Cross Border Privacy Rules (CBPRs) and that aimed to facilitate transfers of personal data within multi-national companies operating in both Europe and the Asia-Pacific. Like BCRs, CBPRs are designed to ensure that a company's privacy policies meet established standards for the protection of personal information. In the instance of CBPRs, such policies must be validated by APEC-recognised Accountability Agents.

The Asia-Pacific Privacy Authorities (APPA) forum comprises privacy regulators from Pacific Rim countries[40] who meet twice a year to share jurisdictional reports and discuss topical issues including privacy and security, cross-jurisdictional law enforcement in the Pacific rim, privacy legislation amendments, and personal data privacy. The Office of the Australian Information Commissioner provides the APPA secretariat.

Another example of a regional group of DPAs that fosters co-operation is the Meeting of Central and Eastern European Data Protection Commissioners. It has issued Declarations of co-operation on more than one occasion. The 16th Meeting took place in Macedonia in 2014. Some non-EU DPAs are members, including those from Russia, Ukraine, Albania, Moldova, Serbia, Montenegro and Bosnia. The Nordic countries (Denmark, Finland, Iceland, Norway, Sweden) collaborate at the regional level: this includes meetings every one or two years between the authorities looking at planning, benchmarking and management, as well as more regular co-operation on case handling and media relations. Co-operation arrangements also

[38] www.apec.org.
[39] Attorney General's Department, "Asia-Pacific Economomic Cooperation privacy", undated. http://www.ag.gov.au/RightsAndProtections/Privacy/Pages/APECprivacy.aspx
[40] APPA's website is located at www.appaforum.org

include a staff exchange programme, although not all authorities have participated in this. The group produced a joint set of questions to Facebook and a joint report.[41]

The Balkan countries cooperate in the context of the Conference of Balkan Data Protection Countries. Participating countries have signed a Declaration of Co-operation, which included the Czech Republic, Slovenia, Albania, Bosnia and Herzegovina, Croatia, Kosovo, Montenegro and the former Yugoslav Republic of Macedonia.

Another example of regional groups is the Baltic cooperation of DPAs (Estonia, Latvia and Lithuania). They have co-operated regionally on two joint supervisions. They also co-operate on monitoring and issuing recommendations. Finally, the members of the Visegrad Group (Czech Republic, Hungary, Poland and Slovakia) work together on areas of common interest within European integration. The group is not institutionalised, but consists of meetings of its representatives at various levels, including ministerial co-operation.

3.6 Language-based networks

In addition to regional networks that foster DPA co-operation, there are also two important language-based networks. One is the Ibero-American Data Protection Network (RIPD), initiated by the Spanish DPA (AEPD), which provides the network's secretariat. The other is the *Association francophone des autorités de protection des données personnelles* (AFAPDP), which promotes co-operation and training between countries that speak French in the area of personal data protection.[42] CNIL, the French DPA, provides the secretariat. It has 27 members from 24 countries.

3.7 Memoranda of Understanding

In addition to the above-mentioned networks of co-operation, DPAs also use specific instruments to foster co-operation and co-ordination, such as memoranda of understanding (MoUs) . Several DPAs have concluded MoUs with the aim of enforcing privacy and data protection laws: for example, the US FTC has MoUs with Spain, the UK and Ireland; the Office of the Privacy Commissioner (OPC) of Canada has MoUs with the ICO and the German Federal Data Protection Commission; the OPC and the Dutch DPA have an MoU, which was the basis for their collaboration in the investigation of WhatsApp. DPAs have also concluded MoUs with aims other than the enforcement of privacy and data protection laws, such as the co-ordination of their policies regarding the enforcement of privacy and data protection laws: for instance, the Macedonian DPA has signed several MoUs with various DPAs.[43]

4 Powers

The second PHAEDRA survey revealed differing powers among DPAs.[44] DPAs that do not have investigation or audit powers, or have weaker sanctions than other DPAs, may not be able to carry their weight in a delegated, multinational investigation. For example, the Belgian DPA lacked the power to fine or censure SWIFT when it transferred Europeans' financial

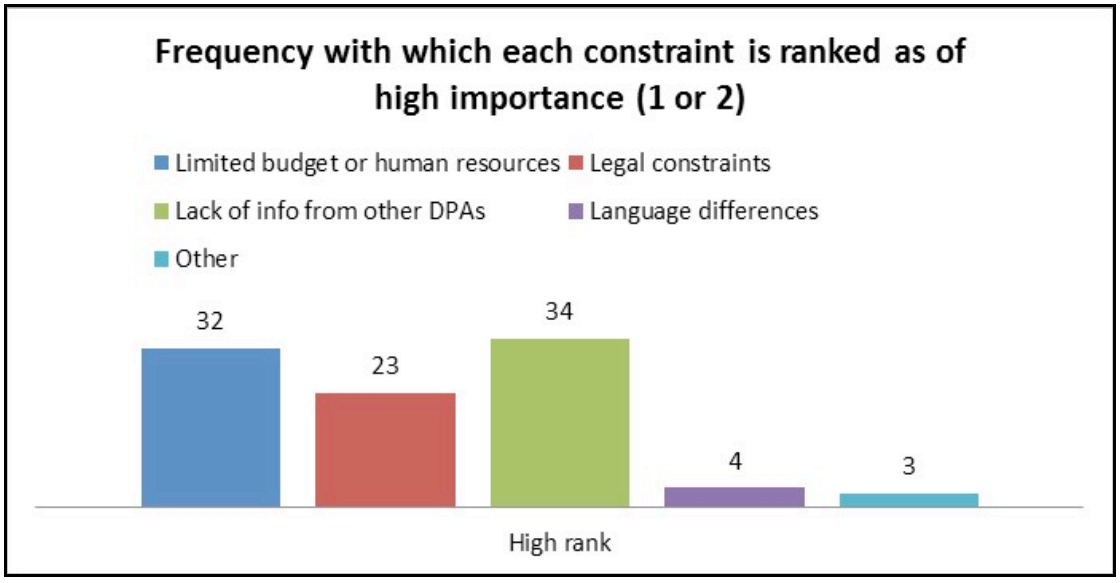
[41] Jonasson, David, "Facebook's data protection questioned by Nordic authorities", Stockholm News, Stockholm, 12 June 2011. http://www.stockholmnews.com/more.aspx?NID=7485
[42] http://www.afapdp.org/
[43] See PHAEDRA project D2.1 deliverable and Annex 2 for more examples.
[44] See Annex 1 for the results of the questionnaire.

transaction data to US authorities in 2006.[45] Other DPAs, e.g. the ICO, CNIL and the AEPD (the Spanish DPA), do have the power to levy monetary penalties and have done so, but the level of fines has varied significantly.

In the EU, the proposed Data Protection Regulation will strengthen the powers of DPAs, so that all will have the power to levy fines of up to five per cent of a company's global turnover.[46]

5 Surveys

In the course of the PHAEDRA project, the consortium conducted three surveys. In mid-February 2013, the PHAEDRA consortium sent out a questionnaire to 79 DPAs around the world. The two-page questionnaire had 10 questions asking about areas for improving co-operation and co-ordination, possible constraints, measures for improving co-ordination of investigations, sharing information, suggestions for case studies and examples of co-operation. The survey elicited 53 responses. Among the findings of the survey were that the chief constraints on achieving more co-operation were limited resources, lack of information from other DPAs and legal constraints, as depicted in the following diagram.



We asked DPAs which measures could be taken in the short term to improve co-operation and co-ordination. Among the responses were:

- MoUs
- A common information platform (a website)
- A repository of data protection acts translated into at least English
- An intranet for DPAs
- Teleconferences (like those conducted by GPEN)
- A small secretariat

[45] The Belgian public prosecutor, which has such a power, decided not to pursue any legal action against SWIFT despite the wishes of the Belgian DPA, and the Opinion of the Art. 29 WP.
[46] See Article 79 GDPR. The EC in its proposal of 25 Jan 2012 for a Regulation called for two per cent, but the European Parliament in its revision of the proposal, adopted 12 March 2014, changed this to five per cent.

- An efficient secure mechanism for authorities to indicate that they are interested in an issue or incident and to determine whether other authorities are interested in working together on a particular issue and forming a group to pursue the matter.

Other measures included information sharing (a pooling of intelligence) on major cross-border cases and issues, including legal assessments and envisaged measures; sharing of best practices; joint case studies, and more resources.

The survey turned up numerous examples of training, staff exchanges and study visits, all of which are manifestations of co-operation. For example, an Austrian DPA representative spent two months in training at CNIL, while another spent several weeks at the Swedish DPA. The Bosnia and Herzegovina DPA has benefitted from "Twinning Assistance to the Personal Data Protection Agency" in co-operation with the Data Protection Commissioner of Saxony (Germany). Canada said it has hosted several delegations over the last few years, including the Commissioner of a newly created authority in the Caribbean who spent several days at the OPC. Canada has also hosted a South African delegation and officials from Burkina Faso and Benin, who spent a week at the OPC. The Office of the Privacy Commissioner for Personal Data of Hong Kong has held training sessions for staff from other DPAs, including from Macao. The Irish DPA has hosted other DPA representatives at its office and gave one DPA inspection powers under its Act in the conduct of an audit. Israel mentioned the AEPD-ILITA twinning program, which was "a successful, enriching and important program that allowed ILITA staff to discuss cutting edge issues with international colleagues". Mexico cited as an example of co-operation the trainings provided by senior officials from the Canadian Privacy Commissioner's Office and the US Federal Trade Commission.

One respondent advocated establishing a higher level of trust and sustaining relationships between DPAs so that they are willing to share information would help improve co-operation and co-ordination in the short term.

The second PHAEDRA questionnaire was issued in October 2013. At the first PHAEDRA workshop held in conjunction with the International Conference of Data Protection and Privacy Commissioners in Warsaw in September 2013, the consortium had a good discussion of issues relating to privacy enforcement co-ordination. However, the consortium did not have sufficient time to discuss one important point on its agenda, which was: how could the PHAEDRA project best support DPAs, PCs and PEAs in its second year? To that end, the consortium developed a list of six possibilities from the many responses received to the first PHAEDRA questionnaire. Based on responses received, the consortium eventually decided on support of the ICDPPC's International Enforcement Co-operation Working Group (IECWG) and identifying barriers to co-operation and ways in which those barriers could be overcome.

After the processing of the first and second survey,[47] PHAEDRA conducted a third survey in October 2014 (see Annex 3 for the responses).[48] From our survey of DPAs and PCs regarding how they find out about investigation and enforcement actions, we draw the following conclusions:

[47] Other findings from the second survey can be found in Annexes 1 and 2.
[48] See annex 3.

- For most DPAs and PCs, they find out about the investigations and enforcement actions initiated by others in a somewhat ad hoc, non-structured process. They learn of such actions by a variety of means, such as through the Article 29 Working Party, GPEN, informally from other DPAs and PCs, through press releases, news items, and at workshops and conferences. The Case-Handling Workshop associated with the Spring Conference in Europe and the International Working Group on Data Protection in Telecommunications (IWGDPT, aka the Berlin Group) are other sources of information.
- Not all DPAs and PCs learn of such actions through all of these means. Indeed, most respondents learned of such actions through only some of these means.
- Bilateral and/or multilateral agreements are another source of information. Checking others' websites is another source, but checking other websites must be regarded as very much of a "hit or miss" process.
- There is some expectation that the GPEN alerting system will provide a more structured means of becoming informed about actions, but that alerting system will be available, of course, to only those DPAs and PCs who are members of GPEN, and not all are members. (GPEN has about 50 members as of December 2014.)
- A further issue re how DPAs and PCs learn of investigations or enforcement actions initiated by others is the timeliness of information, i.e., when some DPAs or PCs learn of such actions, it may already be too late for them to participate or contribute to such initiatives. Nevertheless, there is no structured reporting mechanism in place so that even where the information is no longer timely, it is not reported to others even as a matter of record.
- Yet another issue is that some DPAs or PCs or PEAs may not be able to share information about investigations or enforcement actions that they have recently initiated or that are on-going.
- Even where a DPA or PC is able to share information about investigations or enforcement actions they have initiated, they must exercise some degree of judgement about which actions they think might be of interest or relevance to others, i.e., they may undertake hundreds of such actions every year, but only a few may be of interest to others.

6 Interviews

In addition to the questionnaire survey sent to 79 DPAs, PHAEDRA conducted 19 one-on-one, in-depth telephone interviews with DPAs, privacy commissioners (PCs) and other privacy enforcement authorities (PEAs) to gain deeper insights into privacy enforcement instruments and views on improving privacy enforcement co-ordination internationally. Among the issues discussed in the interviews were the following:

- Differences in powers
- Sharing confidential information
- Art. 29 WP and APEC
- The International Conference and GPEN
- An ICDPPC website and secretariat
- A lead DPA in investigating issues of concern to multiple DPAs
- Complaints
- Instruments for enforcing privacy
- Actions to improve co-ordination globally

- Challenges to improve enforcement co-ordination
- Privacy, security and consumer protection

The interviews were helpful in understanding better DPAs' enforcement powers, the challenges they face in privacy enforcement co-ordination and the efforts they are making to overcome those challenges. The interviews were also helpful to PHAEDRA in determining what actions the consortium should take in supporting DPAs in the context of Work Stream 3.

7 Barriers to co-operation and co-ordination

Despite good will among DPAs, they still face various barriers to co-operation and co-ordination, some of which are described below.

7.1 Confidentiality and legal barriers

The task of effective international enforcement outside of Europe is complicated by the absence of internationally accepted data protection standards and the potential conflict with the confidentiality obligations laid down in Article 28.7 of the Directive and Article 15 of the Convention 108.[49]

From interviews with DPAs, it is clear that DPAs have discussed at length the issue of how far they can go in releasing confidential information (not personal data) to their counterparts in other countries, even if doing so would contribute to apprehending large companies who are not troubled by their compromising privacy. Existing legislation enabling the DPA or privacy commissioner or PEA may prevent or hamper the sharing of information. Laws have differences in scope from one country to another, i.e., there are differences in DPA powers.

Best elements for reducing the various barriers to global co-operation and co-ordination are discussed further below (under 8.3).

7.2 Lack of resources

From the first survey undertaken by PHAEDRA, the consortium found that most DPAs have fewer than 60 staff. Only a few have more than 60 staff members. However, one DPA responded to our questions with the comment that "there is a solid amount of non-used resources and opportunities to improve the international and domestic work of DPAs". Nevertheless, a shortage of resources can affect even DPAs with larger staff. From the interviews conducted by the PHAEDRA consortium, we learned that one DPA may ask another DPA for some support, for some information, some action and a response may go unanswered for some time. Many DPAs favour some time limits in an international privacy enforcement co-ordination arrangement governing the amount of time before a response to a request is due.

Berlin DPA Alexander Dix has highlighted the problem (the challenge) of resource shortages, with the following example:

> The Facebook case has highlighted a more generic problem of enforcing privacy rules against global players. The office of the Irish Data Protection Commissioner is undoubtedly

[49] Hawkes, Billy, "Data protection enforcement challenges facing smaller DPAs", in David Wright and Paul De Hert (eds.), *Enforcing Privacy*, Springer, Dordrecht, 2015 [forthcoming].

> understaffed[50] compared to other European jurisdictions such as France or Germany. This may have influenced the decision of Facebook and other US providers such as Google and LinkedIn to have their European headquarters in Ireland although other considerations (e.g., tax legislation) could well have played a more prominent role in this decision. It is obvious that auditing large companies such as Facebook strains the scarce resources of a small data protection authority to its limits. The Irish Commissioner's audit of Facebook led to some changes in the service of the company, e.g., in the field of face recognition. However, basically the Commissioner accepted the argument brought forward by Facebook that users had no choice but to pay for the service with their personal data. Without disputing that this was a correct interpretation of Irish law, the example shows two major deficiencies in transnational enforcement: as long as the material rules on data protection as well as the resources of data protection authorities differ even within Europe, there is considerable room for *forum shopping* for companies (European or non-European).[51]

The proposed Data Protection Regulation should reduce or eliminate the risk of forum shopping and may help with regard to the resources constraints faced by DPAs, but it is unlikely to eliminate the latter challenge altogether.

7.3 Variability in technical resources

Because many DPAs have limited staff, they do not have the range of competencies needed to address many of the main challenges facing DPAs today. In some cases, as in Ireland, the DPA is able to recruit external expertise on a short-term basis.

7.4 Lack of awareness

In response to a PHAEDRA survey, some DPAs mentioned the difficulty of knowing "what's going on" or "what's happening". Their limited human resources are a factor in some DPAs having an imperfect understanding of the principal issues being discussed in the ICDPPC or GPEN or the Art. 29 Working Party or the IWGDPT. Some DPAs said they might like to participate in a co-ordinated privacy enforcement initiative, but weren't always aware when such initiatives were being taken, or who was the lead DPA and how they might be able to contribute to the collective effort.

The UK ICO said there is lack of understanding about the legal provisions across the world about what can and cannot be shared before, during and after enforcement action. Whilst GPEN and, in Europe, the case handling workshop are helping to address this issue, lack of awareness is still an issue for various DPAs.

7.5 Language capability

There are 24 official languages in the EU, but most international meetings are conducted in English, which is more or less the lingua franca. Even so, some DPAs have difficulty expressing themselves in English, which limits their ability to contribute effectively, to speak cogently at meetings and to prepare written contributions, no matter how earnest and desirous they are of doing so.

[50] The office had 30 members of staff at the time of the Facebook audit, with no legal expert among them.
[51] Dix, Alexander, "The International Working Group on Data Protection in Telecommunications – contributions to transnational enforcement", in David Wright and Paul De Hert (eds.), *Enforcing Privacy*, Springer, Dordrecht, 2015 [forthcoming].

7.6 Lobbying power of multinationals

Multinationals have been rather successful in watering down the proposed Data Protection Regulation,[52] although they have not (yet) got everything they wanted. The biggest multinationals such as Google and Facebook pour huge resources in lobbying against provisions with which they disagree and bring to bear the US government to support their efforts. To the extent that Silicon Valley is successful in watering down the provisions of the proposed Data Protection Regulation, it reduces the prospects for improved privacy enforcement and, with it, more effective co-ordination between DPAs.

7.7 Recognition of PEAs

In the last few years, the term "PEA" (privacy enforcement authority) has come into currency. There are differences between data protection authorities, privacy commissioners and PEAs. The ICDPPC nominally accredits only those "autonomous" institutions that are not under the direction of a government ministry. Ideally, the DPA should be authorised and funded by Parliament. The GPEN is not so strict. DPAs, PCs and PEAs can all become members of the GPEN. To the extent that the ICDPPC has stricter accreditation rules than GPEN, it limits the prospects for co-operation and co-ordination with PEAs that are so autonomous as those accredited by the ICDPPC.

As the types, powers and resources of DPAs, PCs and PEAs vary considerably, some authorities often cannot engage in co-operation with their peers. This is because laws, especially in Europe, prevent performing some enforcement functions with authorities that *do not* fulfil the criteria of independence. In other words, European DPAs that are independent due to the EU legal framework,might not jointly investigate a case with counterparts in jurisdictions that donot impose independence as a condition for a DPA, PC or PEA.

7.8 The Snowden revelations

Since June 2013, the Snowden revelations have become a standing, ongoing topic of discussion among DPAs. The revelations have raised many issues, many of which are still active (e.g., the Safe Harbor agreement). While the Snowden revelations are not a barrier as such for privacy enforcement by DPAs, they nevertheless have raised many issues[53] that challenge even more the limited resources – and independence – of some DPAs. To the extent that the revelations place greater demands on DPA resources, they indirectly impact DPA resources that might otherwise have been devoted to improving co-ordination. The Snowden revelations have also shown the limitations of DPAs in providing oversight of the intelligence agencies and their violation of citizens' fundamental rights.

---

[52]See the chapters by Jacob Kohnstamm and Jan Albrecht Phillips in David Wright and Paul De Hert (eds.), *Enforcing Privacy*, Springer, Dordrecht, 2015 [forthcoming].

[53] See especially the European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230. See also the European Parliament Committee on Civil Liberties, Justice and Home Affairs (the "LIBE committee"), Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), 21 February 2014. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN

8 Findings from the PHAEDRA legal analysis

From its legal analysis, the PHAEDRA team developed several key findings as follows:

8.1 No well-developed legal framework for global co-operation between DPAs

There is no traditional legal framework (e.g., a convention or agreement) that organises global collaboration between DPAs. Despite this lack of a well-developed legal framework for co-operation between DPAs, a significant number of networks between DPAs have emerged.[54] It can be expected that such networks will continue to address co-operation between DPAs and set the pace for co-operation between non-neighbouring countries.[55]

8.2 Various forms and aims of co-operation between DPAs

Co-operation between DPAs can take various forms, involving personal data exchanges or not. At least three distinctive forms of co-operation can be identified:

1. Soft forms of co-operation
   - raising awareness, aimed at informing and educating the public about privacy and data protection laws;
   - assistance between DPAs for the purpose of establishing or strengthening the institutional framework of DPAs, or to support other DPAs with the implementation of privacy and data protection laws.
2. Hard forms of co-operation (enforcement of privacy and data protection laws).
3. Co-operation aimed at setting standards (between soft and hard aims of co-operation).
   - An example of standard setting is evident in a Working Document of 26 November 2014, in which the Art. 29 WP sets forth a co-operation procedure between DPAs for issuing common opinions on contractual clauses considered as compliant with the EC model clauses.[56] The Art. 29 WP wants to preclude the risk that DPAs come to different conclusions when analysing compliance of (national) contractual clauses with the same (EC) model clause.
   - A second example of standard setting is the co-operation between DPAs for interpreting judgments of the European Court of Justice (ECJ). In September 2014, the Art. 29 WP discussed the follow-up to the *Costeja* ruling of the ECJ of 13 May 2014, which acknowledged the right to be de-listed from search engine results. The European DPAs agreed on a common 'tool-box' to ensure a co-ordinated approach to the handling of complaints resulting from search engines'

[54] See above, section 3.

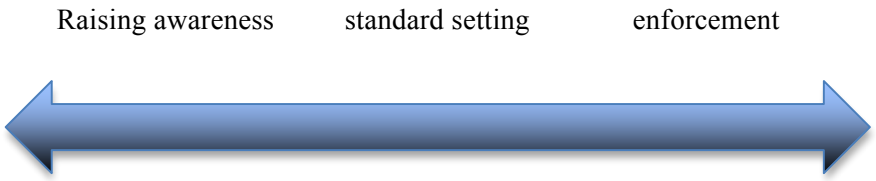
[55] On 2-3 April 2014, the Central and Eastern Europe Data Protection Authorities (CEEDPA) adopted a "Declaration on mutual assistance and enhanced cooperation", declaring their aim "[t]o provide mutual assistance for ensuring an adequate implementation level of personal data protection in *our* countries" (italics added). Central and Eastern Europe Data Protection Authorities, "Declaration on mutual assistance and enhanced cooperation", Skopje, 2-3 April 2014.
http://www.ceecprivacy.org/download/Declaration_on_mutual_assistance_and_enhanced_cooperation.pdf

[56] Article 29 Data Protection Working Party, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" Considered as compliant with the EC Model Clauses, 26 November 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf

refusals to 'de-list' complainants from their results.[57] A List of Common Criteria for Handling Complaints was included in the Art. 29 WP's Opinion of 26 November 2014 on the implementation of the *Costeja* judgment.[58]

Hence, co-operation can be depicted as spectrum as shown in the figure below.

Figure 1: from soft co-operation to hard co-operation



The following forms of co-operation apply to the three kinds of co-operation:

- monitoring privacy and data protection laws in other countries; sharing of standards and information
- training and staff exchanges
- possibilities to carry out projects to improve co-operation.

The following forms of co-operation apply to enforcement co-operation:

- mutual legal assistance;
- parallel or joint investigations;
- mutual recognition; and
- unco-ordinated and non-confidential (see also above on active modes of cooperation, 3.1)– this type of ad-hoc information sharing is permitted legally but not within the context of a specific case as such, but still contributes to enforcement capacity-building, e.g., sharing between DPAs of general research about enforcement, or how a DPA reacted in another country to a particular high-profile case – this is already done through GPEN teleconferences.

8.3 Best elements for reducing various barriers to effective co-operation and co-ordination

The PHAEDRA D2.1 deliverable distinguishes best elements for strengthening co-operation between DPAs from general privacy and data protection legislation, establishing legislation of DPAs, networks of DPAs and agreements between DPAs. It can be said that the lack of these elements in a co-operation framework for DPAs poses barriers to their co-operation. A first set of best elements pertains to various aims of co-operation. A second set of best elements concerns the enforcement of privacy and data protection laws.

[57] Article 29 Data Protection Working Party, Press release, 18 September 2014. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140918_wp29_press_release_97th_plenary_cjeu_google_judgment__17sept_adopted.pdf

[58] Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 26 November 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

Best elements pertaining to various aims of co-operation include following points:

- First, the binding nature and the specification of the scope of application of a co-operation instrument (e.g., areas of co-operation, co-operation with actors other than DPAs, co-operation with non-EU DPAs, forms of co-operation such as spontaneous information exchanges and staff exchanges, and categories of information such as sensitive information). For instance, on 9 October 2014, German DPAs adopted a Resolution on stronger co-operation with competition law authorities.[59]
- Second, privacy and data protection legislation or co-operation instruments should provide strong legal anchor points for various aims of co-operation, such as the independence of DPAs[60] and a legal basis for co-operation.
- Finally, best elements pertaining to various aims of co-operation include technical tools for co-operation (e.g., templates for co-operation requests and the development of an e–platform[61]), a set of evaluation tools (e.g., a timeline for co-operation and audits) and the use of other co-operation mechanisms (e.g., agreements with other DPAs).

Best elements pertaining to enforcement co-operation include following points:

- First, the scope of application of a co-operation instrument (e.g., the different phases of an enforcement case, the different types of infringements, the actors of infringements and categories of information such as information on investigative techniques).
- Second, privacy and data protection legislation and co-operation instruments should provide strong legal anchor points for enforcement co-operation, such as the one-stop shop and consistency mechanism discussed in the proposed General Data Protection Regulation, the clarification of the cross-border investigatory powers of DPAs and the specification of the limitation grounds for co-operation between DPAs (e.g., the exchange of personal data, refusal grounds for co-operation, consent of the data subject).

[59] Hunton & Williams LLP, "German DPAs Adopt Resolutions Regarding 'Connected Cars' and Co-operation with Competition Authorities", Privacy and Information Security Blog, 20 October 2014. https://www.huntonprivacyblog.com/2014/10/articles/german-dpas-adopt-resolutions-regarding-connected-cars-cooperation-competition-authorities/

[60] The independence of DPAs is required in Article 16 of the Treaty on the Functioning of the EU, Article 8 of the Charter of Fundamental Rights of the EU, and Article 28(1) of Directive 95/46/EC. The Court of Justice of the EU (CJEU) has passed three judgments finding a lack of independence of DPAs: CJEU (Grand Chamber), Case C-518/07, *European Commission v. Germany*, 9 March 2010; CJEU (Grand Chamber), Case C-614/10, *European Commission v. Republic of Austria*, 16 October 2012; CJEU (Grand Chamber), Case C 288/12, *European Commission v. Hungary*, 8 April 2014. Furthermore, the European Agency for Fundamental Rights (FRA) has repeatedly recommended that "the independence of DPAs must be strengthened through a reform of EU legislation": European Agency for Fundamental Rights, "Access to data protection remedies in EU Member States", Luxembourg, Publications Office of the European Union, 2013, p. 9. http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states. See also: European Agency for Fundamental Rights, "Data Protection Authorities in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II", Luxembourg, Publications Office of the European Union, 2010, 50 pp.

[61] For instance, in September 2014, the Art. 29 WP followed up on the *Costeja* ruling of the ECJ. The Art. 29 WP decided "to put in place a network of dedicated contact persons in order to develop common case-handling criteria to handle complaints by the data protection authorities. This network will provide the authorities with a common record of decisions taken on complaints and a dashboard to help identify similar cases as well as new or more difficult cases." See Article 29 Data Protection Working Party, Press release, 18 September 2014. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140918_wp29_press_release_97th_plenary_cjeu_google_judgment__17sept_adopted.pdf

8.4 Global Cross-Border Enforcement Co-operation Arrangement

As said above (under 3.4), the 2014 International Conference in Mauritius adopted a Resolution on a Global Cross-Border Enforcement Co-operation Arrangement. Although the Arrangement is a valuable multilateral tool to facilitate confidential sharing of enforcement related information, it is not intended to create binding obligations or replace existing regional mechanisms for co-operation and information sharing. Rather, it aims to foster a coalition of the willing. It is open to Conference members and "partners": Convention 108 signatories, GPEN members, Art. 29 WP members and APEC CPEA members.

8.5 More oversight by DPAs of intelligence services

On November 2013, the Belgian DPA and Dutch DPA initiated a co-investigation into the security of the financial system of the Society for Worldwide Interbank Financial Telecommunication (SWIFT), following alleged access by foreign intelligence services to SWIFT's financial data traffic.[62] On 28 January 2014, the Canadian DPA (OPC) launched a report calling for more oversight of the Canadian intelligence services.[63] It could be questioned to what extent DPAs co-operate regarding the oversight of cyber-surveillance and intelligence gathering agencies. Furthermore, following the 2013 Snowden revelations, on 10 April 2014, the Art. 29 WP adopted an Opinion on surveillance of electronic communications for intelligence and national security purposes, in which it recommended, among other things, "[e]ffective, robust and independent external oversight, performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself, having power to access data and other relevant documentation on a regular basis and on its own initiative (ex officio), as well as an obligation to inspect following complaints".[64]

9 Benefits for Europe of international co-operation

This section summarises the benefits for Europe of International co-operation and co-ordination. Individual DPAs have recognised the benefits (and necessity) of international co-operation in responding to privacy issues that cross borders.

9.1 Better observance of the fundamental rights to privacy and/or personal data protection

From the broadest perspective, enhanced, effective and efficient co-operation of DPAs, PCs and PEAs ensures better observance of the fundamental rights to privacy and/or personal data protection, which had been recognised in the constitutional systems of virtually all Western liberal democracies. At the end of the day, it benefits the individuals ("data subjects" in

[62] Gardner, Stephen, "Belgian, Dutch DPAs Find No Evidence of Unlawful Surveillance of SWIFT System", 12 May 2014. http://www.bna.com/belgian-dutch-dpas-n17179890390/. Boulet, Gertjan, and Elonnai Hickok, "Post-Snowden reactions in India and Belgium: A snapshot", Jusletter IT. Die Zeitschrift für IT und Recht, 2014, Issue 24, p. 6. http://jusletter-it.weblaw.ch/en/issues/2014/15-Mai-2014.htmlprint

[63] Office of the Privacy Commissioner of Canada, "Canadian Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance", 28 January 2014. https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp

[64] Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 April 2014, 819/14/EN WP 215, p. 13. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

European terminology), offering them a higher level of protection and enforcement of their rights.

9.2 Prevent regulatory arbitrage

Co-ordination in enforcement actions helps ensure that data controllers are not able to shop for the most favourable regulatory regime. It also prevents data controllers from claiming that an issue has already been investigated on the basis of an unsatisfactory investigation, potentially conducted by a DPA with limited or no capacity for sanctions or fines.

9.3 Harmonisation of privacy enforcement

Similarly, increased co-ordination and co-operation between DPAs within Europe, including the sharing of best practices and legal reasoning, contributes to the harmonisation of the practical activity of DPAs. This would mean that data controllers would know better what to expect from their interactions with DPAs and not have to deal with a wide range of different methodologies and approaches. This would have benefits for the common market.

9.4 Expand European model of privacy and data protection

The activity of the Art. 29 WP has been identified as particularly influential and a model of good practice for co-ordination, even by DPAs beyond the EU. If the EU is able to offer strong lessons and best practice, based on its experience in data protection activity and privacy enforcement, then this offers a potential for the expansion of the European model of privacy and data protection beyond the borders of the EU, as other countries work with EU DPAs and potentially learn from them. There are, of course, limits to this process based upon national privacy and data protection regimes.

9.5 Protect Europeans in third countries

Co-operation and co-ordination help ensure that Europeans are protected in third countries. By building relationships with non-European DPAs and equivalent organisations, European DPAs acquire avenues for communication and interaction that can be used to ensure that the data protection rights of European citizens are not infringed.

9.6 Raise overall standard of privacy protection

Finally, co-operation should help raise the overall standard of privacy protection. More resources can be brought to bear more efficiently on particular investigations and issues. Additionally, different perspectives on these issues can be illuminative, increasing the collective expertise of the privacy protection community.

10 Findings and recommendations

In this section, we bring together the findings from this study and then present recommendations on improving co-operation and co-ordination for privacy enforcement.

While DPAs face formidable challenges, nevertheless, they are making progress in improving co-operation, as evidenced by the growing success of GPEN and the Resolutions of the ICDPPC. The Arrangement agreed in Mauritius was a major accomplishment, especially as it

went through 16 versions before agreement on the text was reached. Furthermore, the number of DPAs is continuing to grow. Since the start of the PHAEDRA project, Japan has established a DPA, the Specific Personal Information Protection Commission.

A major issue is lack of understanding about the legal provisions across the world about what can and cannot be shared before, during and after enforcement action. Whilst the Global Privacy Enforcement Network (GPEN) and the case-handling workshop in Europe address this issue, lack of awareness still exists within DPAs. Legal gaps need to be identified in conjunction with developing a framework for information exchange.

One DPA commented in a response to a PHAEDRA survey that the best way to improve cross-border co-operation is for privacy enforcement authorities to seek opportunities for practical co-operation, even where the ability to co-operate remains subject to legal and resource-related constraints. Any effort will provide experience, which, in turn, will help authorities identify and inform any legal and logistical improvements needed. Better understanding of authorities' differing confidentiality requirements in non-public investigations could improve cross-border information-sharing and co-operation. We agree and can recommend this too.

The case studies conducted by PHAEDRA show that privacy enforcement co-operation has occurred, and appears to be increasing in both frequency and level of organisation. However, this collaboration remains primarily in ad hoc forms. Co-operation ranges from full joint investigations to shared inquiries and letter-writing. The most common mode of European co-operation for individual investigations is the identification of the DPA with appropriate jurisdiction, then delegating the leadership for any collective response to this authority. Similarly, group investigations tend to be formed by "coalitions of the willing".

The EU, OECD and APEC have particular influence in this field. The Art. 29 WP plays a strong role in European collaboration. More generally, the European network of overlapping mechanisms for co-operation provides a range of options for collaboration and the building of consensus at different levels and to different purposes. It provides European DPAs with a degree of flexibility in forming different coalitions. Regular interaction may be supportive of developing habits of communication, co-operation and co-ordination. International networks are generally voluntary and not legally binding. GPEN is a relatively new development, which has demonstrated some initial successes. It is a non-binding network for co-operation between privacy enforcement authorities, with an open, potentially global membership and some organisational support from the OECD.

DPAs generally appear interested in learning from the experiences of other DPAs and engage in informal ad-hoc consultation and "watching with interest" (see also the fourth bullet before Finding 5 above). There is a core group of DPAs, many of whom are located in European Member States, who are involved in almost all of the co-operative arrangements available to them. These are also the DPAs with the most resources and the most staff. Encouraging networking amongst these DPAs is therefore not particularly problematic, and it may be worthwhile their dedicating more effort to help bring the smaller DPAs up to their level. These DPAs might, however, be expected to play a leadership role in expanding the opportunities for co-operation and co-ordination to other DPAs outside of this "core".

A lack of situational awareness of the international privacy enforcement context is a key barrier to effective co-operation. DPAs identified a lack of information from their peers about

co-operation and co-ordination activities. This highlights the important role that centralised groups with regular channels of communication can play.

Based on its research and analysis, including from our surveys of and interviews with DPAs, we present the following summary of suggested measures to improve co-operation and co-ordination.

Recommendation 1

Both Member States and EU lawmakers should create an adequate legal framework in internal law allowing their DPA's to engage in EU, European and international co-operation.

Member States should update their national legal provisions clarifying the rights and duties of DPAs faced with needs or demands to co-operate. At the EU level, the proposed Article 45 GDPR, on 'International co-operation for the protection of personal data', and Article 55 GDPR, on 'Mutual assistance' are important steps towards this goal. However, these provisions are rather limited and do not address the reality of MoUs between DPAs, and do not recognise existing networks of co-operation between DPAs. Furthermore, Articles 45 and 55 GDPR should set forth an obligation to safely transmit and safeguard data,[65] and provide safeguards for the exchange of confidential information. Rights of data subjects should also be strengthened, and grounds for refusal of co-operation should be spelled out. In that regard, it is noted that the propositions for modernisation of Convention 108 include a provision on "unambiguous, specific, free and informed" consent for the exchange of personal data between DPAs.

Recommendation 2

DPAs should have the power to directly award damages and impose fines and a broader mandate to share information.

Achieving this goal would generally require new legislation. A collective declaration by DPAs seeking such an outcome might be helpful to this end. The draft EU Data Protection Regulation (GDPR) could be cited by non-EU DPAs that they require similar powers. Although Article 45 of the GDPR is on international co-operation, it may be necessary for national authorities to widen (or deepen) that provision in national law to facilitate a fruitful exchange of information among DPAs without breaching confidentiality rules, which should also provide the legal basis for enforcing procedures or measures initiated by other DPAs.

We also recommend that DPAs seek amendments to their statutory powers so that they have stronger powers to conduct investigations, especially unannounced investigations, and audits and stronger powers of sanction, e.g., in levying stiff monetary penalties, such as those foreseen in the GDPR.

[65] Cf. the International Conference in 2014 adopted a Resolution on enforcement cooperation, encouraging members "[t]o support the development of a secure international information platform which offers a 'safe space' for members of the International Conference and their partners to share confidential information". International Conference of Data Protection and Privacy Commissioners, Resolution on enforcement co-operation, 36th Conference, Mauritius, 2014. http://www.privacyconference2014.org/media/16605/Resolution-International-cooperation.pdf

We further recommend that DPAs (if not the PHAEDRA consortium, which has a fixed duration) continue with carrying out case studies on instances where they collaborate and where collaboration could drive best practices.

Recommendation 3

The European Union should develop co-operation mechanisms with other regional and international stakeholders, in particular the Council of Europe (CoE) as well as networks and associations of DPAs, PCs and PEAs.

As privacy and personal data breaches (torts, contraventions, crimes), due to recent technological developments, often do not stop at the frontiers of a single jurisdiction, there is a critical need for an effective and efficient cross-border co-operation of relevant authorities, especially since there are fundamental rights at stake. However, such cross-border co-operation should be geographically as broad as possible.

In the light of existing instruments and mechanisms of co-operation that themselves are under a process of continuous development, the European Union should assess, approach and develop means of co-operation with other regional and international stakeholders. These would include:

- Council of Europe and its Convention 108, currently under modernisation, which specifically addresses the question of co-operation; it also calls for a "network" of DPAs to be developed;
- Associations of DPAs, PCs and PEAs, such as the Iberoamerican network of DPAs.

While assessing and developing means of co-operation, due diligence should be given to the legal status, powers, competences and duties of these bodies. These could be achieved by further elaborating on Article 45 GDPR, which – should the EU constitutional provisions allow so – could be supplemented by a delegated or implementing act. Delegated acts may be a useful tool to provide clarity on the nature of a co-operation instrument. Article 290 § 1 of the Treaty on the Functioning of the European Union provides that "[a] legislative act may delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act".[66]

Recommendation 4

The European Commission should play an active role in the development of a co-operation framework for DPAs.

The European Commission should actively support the use of the Global Cross-Border Enforcement Co-operation Arrangement. The Arrangement, adopted in the form of a Resolution during the 2014 International Conference in Mauritius, is a valuable multilateral tool to facilitate confidential sharing of enforcement enforcement-related information, but is not intended to create binding obligations or replace existing regional mechanisms for co-operation and information sharing. Furthermore, the arrangement's exclusive focus on enforcement co-operation may pose barriers to its practical relevance in other contexts beyond

[66] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47-390.

enforcement co-operation where the best elements for cooperation in general should be considered.[67]

The practical experiences of spam authorities in the implementation of the Co-operation procedure concerning the transmission of complaint information and intelligence about spam", may provide valuable lessons for implementation by DPAs of a wider Co-operation Arrangement.

Recommendation 5

Privacy and data protection legislation and co-operation instruments for DPAs should distinguish and promote forms and aims of co-operation, and best elements for co-operation between DPAs.

Member States should not only implement the relevant provisions on co-operation under the EU data protection reform but also update their national privacy and data protection laws to reflect the forms and aims of co-operation, and best elements for co-operation.[68] A key best element is the provision of a national legal basis for co-operation, for instance, via creating an obligation to designate an authority or department for the purposes of co-operation.

These forms of co-operation and examples of best elements of co-operation could usefully be included on the platform mentioned in Recommendation 10 below.

Recommendation 6

DPAs should address and clarify the issues of jurisdiction and applicable law at the global level.

While the GDPR addresses the issue of jurisdiction with the one-stop shop and consistency mechanism, the issue needs to be addressed internationally too. Enforcement in the online environment continues to be a challenge, particularly in relation to jurisdiction issues. Sharing between DPAs of legal reasoning relating to how DPAs establish jurisdiction in matters relating to global data flows seems desirable.

Recommendation 7

DPAs should contribute to the development of a central accessible database of the foundation legislation granting DPAs their authority and powers, translated into common languages.

Such a database would allow participants in co-operative exercises to understand the capacities of their partners. The PHAEDRA project D2.1 deliverable has collated legal provisions that both facilitate and impede co-operation and co-ordination.

Recommendation 8

DPAs should increase the number of DPAs involved in co-ordinated expressions of shared concern.

[67] See above, sections 3.4 and 8.3.
[68] See above, section 8.3.

As an example, while seven DPAs sent a letter in 2014 to Insecam, which describes itself as "world biggest directory of online surveillance cameras", other DPAs probably would have been willing to sign the letter too. On the other hand, some DPAs not wish to participate in a particular action because they are of the view that a different strategy (e.g., public education) might be more effective.

In this regard, it would be helpful to have an up-to-date directory of all DPAs, including not only the privacy commissioners, but also those responsible for international relations and enforcement actions. The PHAEDRA consortium could contribute to this effort in context of PHAEDRA. See also the next recommendation.

Recommendation 9

DPAs should develop a single, central, comprehensive list of contacts at other DPAs, preferably a contact list available to all DPAs.

The purpose of a comprehensive list would be to enable individual DPAs to know whom they could or should contact in the event of a need, such as for information gathering or exploring the possibility of an enforcement co-ordination action. Such a contact list should not only include the top official (the DPA or privacy commissioner), but key staff, especially those in charge of international relations and enforcement.

The challenge for such a list or directory or Who's Who is to keep it up to date. After PHAEDRA, this could be maintained by a DPA or the European Commission or the EDPS in its role as secretariat to the new European Data Protection Board or by GPEN. To keep such a directory up to date, it is obviously important that there be a single point of contact who could be notified of any changes in key contacts.

While various DPAs have commented on the need for such a directory over the duration of the PHAEDRA project, some contact lists do already exist, such as that maintained by PHAEDRA as well as other such as APEC, OECD, the Council of Europe and GPEN.[69]

Recommendation 10

In the context of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), DPAs should develop an online platform for sharing information and providing different types of documents (resolutions, criteria, guidelines, regulations).

Many DPAs have expressed the need and wish for an online platform (like that operated by GPEN) for sharing information that, inter alia, could provide a function like a library to help DPAs find different types of documents on various topics of interest. The platform could serve as a discussion forum accessible to all DPAs, could be organised to help DPAs to communicate easily and receive responses quickly. The platform could provide a legal database where each DPA could share decisions with others. Such a legal database would help avoid divergent decisions about the same matter. Such a platform would need to be secure in order to protection confidential information and to encourage open discussion between participants. It would also need to have layered access controls so that DPAs could share information with appropriate participants only.

[69] See above, section 3.4 on mechanism for co-operation at the global level.

Recommendation 11

DPAs should provide a repository of best practice which would allow them to learn from their international peers.

Best practices could expand beyond privacy enforcement to include media and public communication, training, technology watch and other areas of interest to DPAs. A repository of best practice should be combined with a discussion forum or commenting system to allow participants to discuss (and challenge) these best practices. Such a repository could form part of the ICDPPC platform mentioned above.

Recommendation 12

DPAs should collectively finance a co-operative infrastructure (including a small secretariat) at the ICDPPC level.

Relying on volunteers to host meetings or manage projects results in discontinuity, the lack of consistent on-going strategies, an undue burden on a handful of leading DPAs, and overall slow progress. Establishing a small international secretariat was seen by some DPAs as a way of facilitating co-ordination and building institutional structures for co-operation. Finding agreement on funding, as well as location, capacity, and the particular role and responsibilities of the secretariat make this a challenging effort.

Recommendation 13

DPAs should develop a common view of the forensic tools used by them in order to have a common technical approach.

Case studies show that DPAs carry out audits and inspections on the same topics and problems but DPAs have different ways and tools to carry out enforcement actions. Sharing how DPAs carry out enforcement in co-ordinated actions has allowed DPAs to learn more about forensic tools used by other DPAs. But, at the same time, it is clearly desirable to have a common technical approach on using forensic tools taking into account the more advanced techniques of DPAs with greater enforcement experience. As well, it could be useful to discuss the power to conduct online inspections, which the CNIL received in 2014.

Recommendation 14

DPAs should continue with short-term study visits, seminars, training and staff exchanges as useful means to gain first-hand experience and knowledge from other colleagues. DPAs should take advantage of and expand existing mechanisms for fostering co-operation.

Global cooperation needs globally open mechanisms. There may also be scope for opening up some existing EU arrangements to third countries authorities. For example, the case-handling workshop of the Spring Conference could be opened up on some basis to authorities from outside the EU.

Recommendation 15

DPAs should renew and strengthen efforts in building bridges (co-operation) with the International Organization for Standardization (ISO).

There seems to be limited interaction between DPAs and the ISO (or, more particularly, the national standards bodies that feed into the ISO) even though the ISO is developing voluntary standards of relevance to DPAs (for example, in regard to privacy impact assessments). DPAs have made some overtures in this direction (e.g., in the Madrid resolution), but they don't seem to have met with much success as yet.[70] We also recommend that the connection between DPAs and other policy-making fora, such as the Word Trade Organization (WTO) and the United Nations Commission on International Trade Law (UNCITRAL), be explored. Harnessing trade and economic discussions to data protection issues may promote these issues as part of the international discussion, in order to create a global policy-making network, like the work done by the Art. 29 WP. The interaction between data protection, information security and cyber-security may have the potential for ripe data protection concepts to break new ground.

[70] DPAs could collectively develop positions that they could then individually promote within their national standards bodies and committees who feed into the ISO.

11 References

11.1 Books

Wright, David, and Paul De Hert (eds.), *Enforcing Privacy*, Springer, Dordrecht, 2015 [forthcoming].

11.2 Contributions in books

Dix, Alexander, "The International Working Group on Data Protection in Telecommunications – contributions to transnational enforcement", in David Wright and Paul De Hert (eds.), Enforcing Privacy, Springer, Dordrecht, 2015 [forthcoming].

Hawkes, Billy, "Data protection enforcement challenges facing smaller DPAs", in David Wright and Paul De Hert (eds.), *Enforcing Privacy*, Springer, Dordrecht, 2015 [forthcoming].

11.3 Articles

Boulet, Gertjan, and Elonnai Hickok, "Post-Snowden reactions in India and Belgium: A snapshot", Jusletter IT. Die Zeitschrift für IT und Recht, 2014, Issue 24, p. 6. http://jusletter-it.weblaw.ch/en/issues/2014/15-Mai-2014.htmlprint

Kloza, Dariusz, and Anna Moscibroda, "Making the case for enhanced enforcement co-operation between data protection authorities: insights from competition law", *International Data Privacy Law*, Vol. 4, No. 2, 2014, pp. 120-138.
http://idpl.oxfordjournals.org/content/4/2/120.full.pdf+html

Kloza Dariusz, Anna Moscibroda and Gertjan Boulet, "Improving Co-operation Between Data Protection Authorities: First Lessons from Competition Law", *Jusletter IT. Die Zeitschrift für IT und Recht*, Weblaw AG, Issue 20,2013. http://jusletter-it.weblaw.ch/magnoliaPublic/issues/2013/20-Februar-2013/2128.HTML

11.4 Reports

European Parliament Committee on Civil Liberties, Justice and Home Affairs (the "LIBE committee"), Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), 21 February 2014. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN

European Agency for Fundamental Rights, "Access to data protection remedies in EU Member States", Luxembourg, Publications Office of the European Union, 2013, p. 9. http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states

European Agency for Fundamental Rights, "Data Protection Authorities in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II", Luxembourg, Publications Office of the European Union, 2010, 50 pp.

OECD, Report on the Cross-Border Enforcement of Privacy Laws, Paris, October 2006, p. 23.

11.5 Deliverables

Deliverable 1 of the PHAEDRA project: Barnard-Wills, David, and David Wright, "Co- ordination

and co-operation between Data Protection Authorities", Brussels, April 2014. http://www.phaedra-project.eu/?page_id=201

Deliverable 2.1 of the PHAEDRA project: De Hert, Paul, and Gertjan Boulet, "A Compass towards best elements for cooperation between data protection authorities", Brussels, 28 February 2014. http://www.phaedra-project.eu/?page_id=201

Deliverable 2.2 of the PHAEDRA project: De Hert, Paul, and Gertjan Boulet, "Legal reflections for further improving cooperation between data protection authorities", Brussels, 9 May 2014. http://www.phaedra-project.eu/?page_id=201

PHAEDRA, "Executive summary of Deliverables 3.1 and 3.2: Contact list of Data Protection Authorities (DPAs) and collaboration with GPEN and the ICDPPC working group", Brussels, January 2015. http://www.phaedra-project.eu/?page_id=201

Deliverable 3.4, "PHAEDRA workshops and final conference", Brussels, January 2015. http://www.phaedra-project.eu/?page_id=201

11.6 EU legal instruments

Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47-390.

Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, OJ C 316, 27.11.1995, pp. 34-47.

Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, (EC) No515/97, OJ L 83, 13 March 1997, pp. 1-16.

Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, 6 March 2002, pp. 1-13.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM(2012) 11 final.

11.7 Case law

CJEU (Grand Chamber), Case C‑ 288/12, *European Commission v. Hungary*, 8 April 2014.

CJEU (Grand Chamber), Case C-614/10, *European Commission v. Republic of Austria*, 16 October 2012.

CJEU (Grand Chamber), Case C-518/07, *European Commission v. Germany*, 9 March 2010

11.8 Press releases

Article 29 Data Protection Working Party, Press release, 18 September 2014. http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140918_wp29_press_release_97th_plenary_cjeu_google_judgment__17sept_adopted.pdf

CNIL, "CNIL orders Google to comply with the French Data Protection Act, within three months", 20 June 2013. http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-comply-with-the-french-data-protection-act-within-three-months/

Gardner, Stephen, "Dutch DPA Concludes That Google Is in Breach of Data Protection Act", *Bloomberg BNA*, 2 December 2013. http://www.bna.com/dutch-dpa-concludes-n17179880411/

GIODO, "Meeting of the Berlin Group, 23-24 April 2012". http://www.giodo.gov.pl/259/id_art/736/j/en/

Hunton & Williams LLP, "German DPAs Adopt Resolutions Regarding 'Connected Cars' and Co-operation with Competition Authorities", Privacy and Information Security Blog, 20 October 2014. https://www.huntonprivacyblog.com/2014/10/articles/german-dpas-adopt-resolutions-regarding-connected-cars-cooperation-competition-authorities/

Jonasson, David, "Facebook's data protection questioned by Nordic authorities", Stockholm News, Stockholm, 12 June 2011. http://www.stockholmnews.com/more.aspx?NID=7485

Office of the Privacy Commissioner of Canada, "Joint Open Letter to App Marketplaces", News, 9 December 2014. https://www.priv.gc.ca/media/nr-c/2014/let_141210_e.asp

Office of the Privacy Commissioner of Canada, 'Canadian Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance', 28 January 2014. https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp

OECD , "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", undated. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Gardner, Stephen, "Belgian, Dutch DPAs Find No Evidence Of Unlawful Surveillance of SWIFT System", 12 May 2014. http://www.bna.com/belgian-dutch-dpas-n17179890390/

11.9 Other publications

Article 29 Data Protection Working Party, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" Considered as compliant with the EC Model Clauses, 26 November 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp226_en.pdf

Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 26 November 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10 April 2014, 819/14/EN WP 215, p. 13. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

Attorney General's Department, "Asia-Pacific Economomic Cooperation privacy", undated. http://www.ag.gov.au/RightsAndProtections/Privacy/Pages/APECprivacy.aspx

Buttarelli, Giovanni, "How could DPAs better co-operate and provide leadership for the future", Spring Conference, Data Protection, Lisbon, 17 May 2013. http://springconference2013.cnpd.pt/wp-

content/uploads/Giovanni-Buttarelli-Assistant-EDPS-%E2%80%93-How-could-DPAs-better-co-operate-and-provide-leadership-for-the-future.pdf

Central and Eastern Europe Data Protection Authorities, "Declaration on mutual assistance and enhanced cooperation", Skopje, 2-3 April 2014. http://www.ceecprivacy.org/download/Declaration_on_mutual_assistance_and_enhanced_cooperation.pdf

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230.

International Conference of Data Protection and Privacy Commissioners, Resolution on enforcement co-operation, 36th Conference, Mauritius, 2014. http://www.privacyconference2014.org/media/16605/Resolution-International-cooperation.pdf

International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy Enforcement Co-ordination at the International Level, Mexico, 2011. http://privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_001_%20Intl_Priv_Enforc_ENG.pdf

OECD, "OECD Questionnaire on the cross-border enforcement of privacy laws", DSTI/ICCP/REG(2006)1, 2006. http://www.oecd.org/sti/ieconomy/37572050.pdf

OECD, Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, Paris, 2006. http://www.oecd.org/sti/ieconomy/38770483.pdf

Organisation for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris, 23 Sept 1980. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. The revised guidelines can be found here: http://www.oecd.org/sti/ieconomy/privacy.htm

Annex 1 – Enforcement powers

Powers of enforcement

	(1) Receiving and investigating complaints	(2) Inspections (or audits), announced in advance	(3) Unannounced inspections	(4) "Naming and shaming"	(5) Orders (you have the power to tell an offending company to "cease and desist", otherwise they will be penalised with a fine or other sanction)
Albania	Have	Have	Have		Have
Australia	Have	Have	Have	Don't have	Don't have, but can apply to a court for an injunction
Bulgaria	Have	Have	Have	Have. Administrative orders, appeals, conclusions of audits and comparative monitorings are published on our website. We can also do proactive disclosure such as media campaigning, public black lists, etc	Have
Denmark	Have	Have	Have	Have	Have
EDPS	Have	Have	Have	Have, not explicitly, but used in practice on basis of transparency	Have
Estonia	Have	Have	Have	Have	Have
Finland	Have	Have	Have	Don't have	Have
Hong Kong	Have	Have	Have	Have	Have
Hungary	Have	Have	Have	Have	Have

	(1) Receiving and investigating complaints	(2) Inspections (or audits), announced in advance	(3) Unannounced inspections	(4) "Naming and shaming"	(5) Orders (you have the power to tell an offending company to "cease and desist", otherwise they will be penalised with a fine or other sanction)
Lithuania	Have	Have	Have	Have	Have
Mauritius	Have	Have	Have	Have	Have
Mexico	Have	Have	Have	Have	Have
Moldova	Have	Have	Have	Have	Have
Netherlands	Have	Have	Have	Have	Have
New Zealand	Have	Don't have	Don't have	Don't have	Don't have
Ontario	Have	Have	Don't have	Have	Have
Singapore	Have	Have	Have	Have	Have
Slovak Republic	Have	Have	Have	Have	Have
Switzerland	Have	Have	Have	Have. We can publish our recommendation with the name of the controller in case of public interest.	Don't have. We can only address recommendation to modify, cease, … processing. The Federal Administrative Court can confirm or invalidate our recommendation. In last instance, the Federal Court can decide.
United Kingdom	Have	Have	Don't have	Don't have	Have
United States	Have	Don't have	Don't have	Don't have	Have

	(6) Fines (which you can impose directly)	(7) Fines by an administrative court or tribunal, i.e., you need to go to court in order to get a fine imposed on a company that is not compliant with the law	(8) Criminal sanctions	(9) What other powers you have to enforce privacy?
Albania	Have	Don't have	In case the violation consists in a crime, the Commission makes the respective report.	Order, Decision, Recommendation and Publication
Australia	Have	Have	Can refer to prosecuting authorities	the power to conduct investigations on its own initiative (not just in response to a complaint)
Bulgaria	Have	Have	Don't have	Issuing compulsory instructions on personal data protection; issuing opinions and permissions in cases foreseen in law, e.g., data transfer to third countries
Denmark	Don't have	Don't have	Have	
EDPS	Don't have	Don't have, but EUCJ can impose measures where required, upon referral	Don't have	See Article 47 of Regulation 45/2001

	(6) Fines (which you can impose directly)	(7) Fines by an administrative court or tribunal, i.e., you need to go to court in order to get a fine imposed on a company that is not compliant with the law	(8) Criminal sanctions	(9) What other powers you have to enforce privacy?
Estonia	Have	Don't have	Have. Some specific wrongdoings like intentional identity theft, disclosure of health information etc are criminal offences	
Finland	Don't have	Don't have	Have	The Data Protection Ombudsman must be heard in preparation of legislation or administrative reforms. The public prosecutor must consult the Ombudsman prior to bringing charges based on violations of the Personal Data Act. Courts of law are obliged to consult the Ombudsman in cases concerning related issues.
Hong Kong	Don't have	Have	Have, but only by court in connection with (7)	
Hungary	Have	Don't have	Don't have	Informing the public

	(6) Fines (which you can impose directly)	(7) Fines by an administrative court or tribunal, i.e., you need to go to court in order to get a fine imposed on a company that is not compliant with the law	(8) Criminal sanctions	(9) What other powers you have to enforce privacy?
Lithuania	Don't have	Have	Don't have	
Mauritius	Don't have	Have	Have	See part III of the DPA 2004 on preservation orders, entry and search, requesting assistance from other authorities.
Mexico	Have	Don't have	Don't have	
Moldova	Don't have	Have	Have	
Netherlands	Have	Don't have	Don’t have, but we can do criminal investigations into a limited number of breaches of law. We always need a DA and a Court to impose any penalties	Strengthened monitoring and/or serious, but ‘informal’ conversations with and writing serious letters to explain the law/possible complications of (future) non-compliance

	(6) Fines (which you can impose directly)	(7) Fines by an administrative court or tribunal, i.e., you need to go to court in order to get a fine imposed on a company that is not compliant with the law	(8) Criminal sanctions	(9) What other powers you have to enforce privacy?
New Zealand	Don't have	Don't have	Don't have	a. Enforceable codes of practice b. Civil orders by tribunal c. Compensation by tribunal d. Commissioner initiated investigations e. Transfer prohibition notices f. Subject access charging determinations (by Commissioner)
Ontario	Don't have	Have	Have	
Singapore	Have	Don't have	Have	
Slovak Republic	Have	The subject who violated the Law may also be held responsible in front of civil, criminal or administrative court	Don't have, but the subject who violated the Law may also be held responsible in front of civil, criminal or administrative court	See section 46 of the Act No. 122/2013 Coll.

	(6) Fines (which you can impose directly)	(7) Fines by an administrative court or tribunal, i.e., you need to go to court in order to get a fine imposed on a company that is not compliant with the law	(8) Criminal sanctions	(9) What other powers you have to enforce privacy?
Switzerland	Don't have	Don't have	Have, but only a criminal court or tribunal can pronounce such sanctions	
United Kingdom	Have	Have	Have	Information notices that require companies to give us information should we require it. We also have powers to enforce non-notification
United States	Don't have	Have, conditionally	Don't have	The FTC can take action when US-based actions harm foreign consumers. The FTC can accept reimbursement for investigative assistance, and can also participate in foreign staff exchanges. Finally, the FTC has power to enter into binding international agreements for mutual legal assistance in consumer protection matters.

Annex 2 – Information sharing and MoUs

	If one DPA asked you for some information in connection with an investigation, would you be able to gather or share it?	Have you signed a Memorandum of Understanding with any other DPA, PC or PEA?
Albania	Yes	Yes, with Albania, Bulgaria, Kosovo, Macedonia, Montenegro, Ukraine
Australia	Yes, conditionally	Yes, with NZ
Bulgaria	Yes	Yes, with Spain, Macedonia, Albania, Kosovo and Montenegro
Denmark	Yes	Yes, with Macedonia
EDPS	Yes, subject to safeguards	No
Estonia	Yes	No
Finland	Yes	No
Hong Kong	Yes	No
Hungary	Yes	Yes, with Macedonia, Ukraine
Lithuania	Yes, except confidential information	No
Mauritius	Yes	No
Mexico	Yes	No
Moldova	Yes	Yes, with Ukraine, Romania
Netherlands	Yes	Yes, with Canada
New Zealand	It depends	Yes, with Australia
Ontario	No	No
Singapore	Yes, conditionally	No
Slovak Republic	Yes	Yes, with Czech Republic, Ukraine
Switzerland	Yes, with limitations	No
United Kingdom	This depends on the DPA requesting the information.	Yes, with Australia, Canada, US and the Dubai Financial Centre regulatory authority
United States	Yes, conditionally	Yes, with Australiia, Ireland, Spain, UK

Annex 3 – How DPAs learn of investigations and enforcement actions

Data protection authorities (DPAs), privacy commissioners (PCs) and privacy enforcement agencies (PEAs) generally suffer from inadequate human and budgetary resources to tackle the challenges facing them with regard to the protection of privacy, including data protection. In order to leverage scarce resources, DPAs, PCs and PEAs recognise the value of co-operation with their peers. Manifestations of such co-operation include training, staff exchanges, multilateral workshops, conferences and meetings, information exchanges and enforcement co-operation and co-ordination.

However, in order for authorities to collaborate in regard to an enforcement action, they need to know who among their peers is initiating or undertaking an enforcement action. On 9 October 2014, Trilateral sent an e-mail to its contact list of DPAs and PCs to ask how they became aware of enforcement actions initiated by other DPAs.

Following is the text of our e-mail:

> In the context of our research in the PHAEDRA project (www.phaedra-project.eu), which we are undertaking for the European Commission, we would be grateful if you could tell us how you become aware of enforcement actions being taken by one or more other data protection authorities (DPAs) or privacy enforcement authorities (PEAs). Do you become aware of such other enforcement actions through
>
> - Art. 29 WP contacts
> - the Global Privacy Enforcement Network (GPEN)
> - Asia-Pacific Economic Co-operation (APEC)
> - informal or formal contacts with other DPAs
> - through press releases issued by other DPAs
> - through contacts at conferences or workshops
> - through stories in news media (including the IAPP newsletters)
> - other means (please specify)?

We received 19 responses, with a good cross-section from "big" (relatively well resourced) DPAs such as those from the UK and US to much smaller DPAs such as those from Macedonia, Bulgaria and Cyprus.

The following spreadsheet shows the responses received.

How does your DPA become aware of international enforcement actions?	through informal contacts with other DPAs	through press releases issued by other DPAs	from Article 29 Working Party contacts	through the Global Privacy Enforcement Network (GPEN)	through the Asia-Pacific Economic Co-operation (APEC)	through contacts at conferences or workshops	through stories in news media (including the IAPP newsletters)	by other means
Bulgaria		Yes	Yes					bilateral co-operation agreements, International Transfers Subgroup (Art29WP)
Canada	Yes	Yes		Yes	Yes	Yes	Yes	
Colombia				Yes			Yes	
Cyprus	Yes	Yes	Yes			Yes	Yes	Statewatch
Czech Rep	Yes		Yes			Yes		
Germany - Berlin	Yes	Yes	Yes			Yes		
Germany - Schleswig-Holstein	Yes	Yes	Yes	Yes	No	Yes	Yes	
Isle of Man	Yes	Yes		Yes		Yes	Yes	
Italy	Yes	Yes	Yes	Yes		Yes	Yes	Case Handling Workshop; Consumer Protection Cooperation System (ref Article 13 of the 2002/58/EC Directive)
Macao, China	Yes	Yes	No	Yes	No	Yes	Yes	
Macedonia	Yes	Yes	Yes			Yes	Yes	DPA and PEA websites
New Zealand	Yes	Yes	No	No	No	No	No	

Poland	Yes	Yes	Yes	Yes	No	Yes	Yes	International Working Group on Data Protection in Telecommunications (IWGDPT), Council of Europe Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD), International Conference of Data Protection and Privacy Commissioners (ICDPPC), Central and Eastern Europe Data Protection Authorities (CEEDPA), others, e.g., Joint Supervisory Authority of Schengen (JSA Schengen), Case Handling Workshop.
Portugal	Yes	Yes	Yes			Yes	Yes	IWGDPT, Case Handling Workshops
Singapore	Yes						Yes	Updates at APPA Forum by other DPAs
Slovak Republic	Yes	Yes	Yes				Yes	
Switzerland	Yes	Yes	Yes	Yes	No	Yes	No	Convention 108 Consultative Committee, Association francophone des autorités de protection des données
UK	Yes	Yes	Yes	Yes		Yes	Yes	IWGDPT, International Enforcement Event, Case handling Workshop, bilateral MoUs
USA	Yes	Yes	No	Yes	Yes	Yes	Yes	

In addition to the direct responses to the question asked, five privacy commissioners elaborated upon their responses as follows:

Canada

We learn of such [investigation and/or enforcement] actions through all of the methods you list – i.e., generally on an ad hoc basis. We have bilateral sharing arrangements with several international authorities, in addition to being a signatory to the APEC CPEA – much of what we learn from (and disclose to) individual authorities about ongoing and confidential enforcement actions is pursuant to such arrangements.

Macedonia

All points you have put as query are as a piece of mosaic; we are all learning from each other when discussing at conferences and at the bilateral, trilateral and multilateral levels. Of course, the work of the Article 29 and membership in different networks has a great impact. Informal contacts benefit from good communication and individually drawn conclusions. Websites published materials, exchanging each other's Guidelines and E-Newsletters are the best way of finding out "What's App" in every DPA or PEA.

New Zealand

We don't tend to learn anything in a systematic way (the planned GPEN Alerts system is set to remedy that but, as a result of delays caused by some of our European partners, the system build is now delayed now until Q2 2015). We learn [of enforcement actions] in an ad hoc way mainly by enquiring of another authority or on occasion by reading a media release from another authority or, occasionally, the Article 29 Working Party or from press reports. Outside the Art. 29 WP, where there is more frequent meetings and the experience may therefore differ substantially, I suspect that our experience is probably typical.

We don't tend to become aware of enforcement actions in APPA meetings as that's not really the point of the forum and at six-monthly intervals, such intelligence would not be timely. Occasionally we will discuss an enforcement item with broad ramifications (e.g., a Google case) but to place it on the agenda, we will tend already to know of others' actions, albeit we might not know what every single authority is doing and might hear something new but that is exceptional, not a routine source of information. In any case, some of the authorities who may be the most active in enforcement and may know the most (e.g., the FTC) will not reveal that they are, or are not, enforcing against a particular company in that kind of informal discussion.

GPEN does not tend to share this kind of information unless already released publicly. So the GPEN platform is a useful network to let all authorities quickly and simultaneously know that a public inquiry has been announced – it is not used to share confidential information that an investigation has commenced. The GPEN Alerts system will enable confidential alerts to be shared in a controlled fashion (in a sense, not unlike Interpol).

Portugal

Most of the time, DPAs are not aware of enforcement actions carried out by others, because there is no report system in place for such actions, at least not in a regular basis or widely enough.

We have knowledge through several channels, such as the Art 29 WP (meetings or country reports), IWGDPT (country reports in telecommunications sector), informal meetings, conferences, Case Handling Workshops, media coverage, data protection dedicated press/newsletters, and so forth.

On the other hand, not all enforcement actions might be worthwhile to share. For example, the PT DPA applies hundreds of fines concerning video surveillance. This activity itself is worthwhile reporting in general (the circumstances, what is at stake usually) but not the individual case. However, a fine of €4.5 million for a telecom operator is surely worthwhile reporting to other DPAs. The same goes for specific inspections for serious breach or audits or the data controller with activity in several European Member States that might experience similar problems or complaints.

United States

The FTC participates in several MOUs that contemplate sharing confidential enforcement related information, including the existence of investigations or anticipated enforcement actions. This includes the APEC CPEA as well as MOUs with the Data Protection Commissioner of Ireland and the UK Information Commissioner's Office. Even without such an MOU in place, we welcome information regarding other authorities' enforcement activity for assistance or other cooperative purposes. The FTC is able to assure confidentiality of such communications.

Annex 4 – List of abbreviations

AEPD	Agencía Española de Protección de Datos
AFAPDP	Association Francophone des Autorités de Protection des Données Personnelles
APEC	Asia-Pacific Economic Cooperation
APPA	Asia-Pacific Privacy Authorities
Art. 29 WP	Article 29 Data Protection Working Party
BCR	Binding Corporate Rules
CBPR	Cross-border Privacy Rules
CIS	Customs Information System
CJEU	Court of Justice of the EU
CNIL	Commission Nationale de l'informatique et des libertés
CNSA	Contact Network of Spam Authorities
CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
CPEA	Cross-border Privacy Enforcement Arrangement
Directive 95/46/EC	Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
DPA	data protection authority
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ESMA	European Securities and Markets Authority
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
GDPR	Proposal for General Data Protection Regulation
GPEN	Global Privacy Enforcement Network
ICDPPC	International Conference of Data Protection and Privacy Commissioners
IECWG	International Enforcement Cooperation Working Group
ISO	International Organization for Standardization
IWGDPT	International Working Group on Data Protection in Telecommunications
JSA	Joint Supervisory Authority
JSB	Joint Supervisory Board
MLAT	Mutual Legal Assistance Treaty
MoU	Memorandum of Understanding
OECD	Organisation for Economic Cooperation and Development
OPC	Office of the Privacy Commissioner of Canada
PEA	Privacy Enforcement Authority

PC	Privacy Commissioner
RIPD	Red Iberoamericana de Protección de Datos
SIS	Schengen Information System
SPDE	OECD Working Party on Security and Privacy in the Digital Economy
SWIFT	Worldwide Interbank Financial Telecommunication
T-PD	Council of Europe Consultative Committee on the protection of personal data (traité protection de données)
UNCITRAL	United Nations Commission on International Trade Law
US FTC	US Federal Trade Commission
VIS	European Visa Information System
WPPJ	Working Party of Police and Justice
WTO	World Trade Organization