It will be a truism to state that globalisation and recent rapid development of information and communications technologies have resulted in increased trans-border personal data transfers and — at the same time — in the elevation of corresponding risks. This phenomenon both has placed the governance of privacy and personal data protection at the international level and has made data privacy violations with cross-border implications much more frequent. As a result, there grew a critical need for stronger, more enhanced and more efficient cross-border cooperation between relevant supervisory authorities, i.e. between those public bodies that are tasked with "the day-to-day protection of data privacy", on whose shoulders "lies the main burden of effective protection". The status quo of such cooperation leaves much to be desired. Nowadays — to ensure an appropriate level of protection of privacy and personal data and to investigate and prosecute violations, should they occur — these supervisory authorities face constraints by way of human and/or budgetary shortages, practical, institutional and legislative set-ups and similar factors. Often, due to the lack of cooperation and coordination, these resource-constrained authorities may also investigate the same privacy issue, which is, in effect, a duplication of effort. For these reasons, policy-makers, authorities themselves and academics — since as early as 2000s — became preoccupied with diagnosing the problem and with the quest for solutions. … The PHAEDRA research project, or "Improving Practical and Helpful cooperation betweEn Data Protection Authorities" (2013–2015), co-funded by the EU under its Fundamental Right and Citizenship Programme, has been aimed precisely to contribute to this debate. … This book is composed of selected interventions made at the final conference of the PHAEDRA project, held on 12 December 2014 in Kraków, Poland. These contributions are preceded by invited comments written by the experts in the field. Each of these papers — in one way or another touching upon various aspects of cooperation between supervisory authorities — contributes to the unambiguous conclusion that the efficiency of such cooperation is an essential element of the effective protection of the fundamental rights to privacy and personal data protection."
ENFORCING PRIVACY:
LESSONS FROM CURRENT IMPLEMENTATIONS
AND PERSPECTIVES FOR THE FUTURE
This book is based on the research project PHAEDRA (Improving Practical and Helpful cooperation between Data Protection Authorities; 2013–2015), co-funded by the European Union under its Fundamental Rights and Citizenship Programme; http://www.phaedra-project.eu. The research consortium is composed by the Vrije Universiteit Brussel (Belgium; coordinator), Trilateral Research and Consulting LLP (UK), Generalny Inspektor Ochrony Danych Osobowych (Polish DPA) and Universidad Jaume I (Spain). The contents are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

This book constitutes Deliverable D5.3 of the PHAEDRA project.
ENFORCING PRIVACY:
LESSONS FROM CURRENT IMPLEMENTATIONS
AND PERSPECTIVES FOR THE FUTURE

edited by
Paul De Hert, Dariusz Kloza
and Paweł Makowski

Wydawnictwo Sejmowe
Warszawa 2015
Table of Contents

Opening letter from Edyta Bielak-Jomaa, Inspector General for Personal Data Protection 7

European and international cooperation in enforcing privacy – expectations and solutions for a reinforced cooperation Wojciech R. Wiewiórowski 9

Introduction Paul De Hert, Dariusz Kloza, Paweł Makowski 13

Part I

PHAEDRA FINAL CONFERENCE: INVITED COMMENTS

On PHAEDRA’s final recommendations: A few “helpful” tips on how “practical” progress can best be made in enforcement cooperation Blair Stewart 19

Cooperation and coordination viewed by supervisory authorities themselves: results of PHAEDRA surveys David Wright, Kush Wadhwa 23

Dealing with overlapping jurisdictions and requests for mutual legal assistance, while respecting individual rights. What can data protection law learn from cooperation in criminal justice matters? Paul De Hert, Auke Willems 49

Towards efficient cooperation between supervisory authorities in the area of data privacy law Dariusz Kloza, Antonella Galetta 77
Part II

PHAEDRA FINAL CONFERENCE:
SELECTED INTERVENTIONS

Agenda of the PHAEDRA Final Conference in Kraków, Poland 111

The Weltimmo case in light of the future General Data Protection Regulation. One-stop-shop – burden or catalyst among cooperating data protection authorities? 113

Endre Győző Szabó

Biometrics in the context of different legal approaches 119

Marek Múčka

Institutional experience from international cooperation and joint investigations 128

Dimitar Gjeorgjievski

Cooperation between personal data authorities: the Moroccan experience 137

Lahoussine Aniss
Ladies and Gentlemen,

The publication you are holding in your hands is an evidence of the two-year work of PHAEDRA project’s partners, devoted to improving practical cooperation between data protection authorities (DPAs). I am both very pleased and proud that the Inspector General for Personal Data Protection of Poland has had an opportunity to take part in this research project.

The principal objective of the project was to diagnose problems hampering cooperation between particular DPAs and to subsequently prepare recommendations aimed at improving this situation. Why is this field of activity so important to us – data protection commissioners – today? More and more risks to privacy of individuals are related to trans-border data transfers. In today’s dynamically developing world, global information flows do not in fact encounter any technological obstacles. Hence, for multinational companies personal data become a commodity in conducting their businesses. Appropriate reaction to related personal data and privacy breaches requires undertaking efficient cooperation between DPAs from various countries. This issue is still perceived as one of the weakest links in personal data and privacy protection management. Therefore, we ourselves have had very high expectations towards this project.

Today, looking at the fruits of this work from the perspective of a DPA, I can say with certainty that they should become one of the main tools for those participating in the process of developing the future EU data protection framework. For this is the main reference point to the objectives that had been set at the commencement of the project. The fast-approaching reform of data protection regulations will introduce serious changes concerning mutual coordination of tasks by European data protection authorities. Such cooperation will no longer be just one of possible options, but will become an obligation resulting from the new EU law. Hence, I believe that the recommendations and conclusions developed by the PHAEDRA partners deserve attentive reading.

Warsaw, June 2015
Foreword

European and international cooperation in enforcing privacy – expectations and solutions for a reinforced cooperation

Wojciech Rafał Wiewiórowski
European Data Protection Assistant Supervisor

Ladies and Gentlemen,

Speaking at the final conference of the PHAEDRA project which united practicing lawyers, regulators and the people from academia in a discussion on how to improve the cooperation between data protection authorities, I would like to discuss two important subjects. One of them I will address from the academic point of view. The other deals with the basics of coordinating the real work of data protection authorities.

Let me start by wearing my “academic hat”. What should the academia expect from the cooperation of data protection authorities? What should we expect from the community of academia? First of all, bearing in mind that members of the academia are very keen on discussing the problems which “may” arise or “will” arise on the market and have a tendency to correct data protection authorities, governmental officers and all other participants to the scheme of cooperation on international level, I would like to say that…

- we do a great job for academia!
- we provide them with more and more material to write about!

Moreover, they are well-prepared to do that. I remember Paul Nemitz¹ from the European Commission talking at the meeting with the members of academia a year ago. He said he knew that professors had already written the

¹ Paul Nemitz, Director for Fundamental rights and Union citizenship in the Directorate-General for Justice of the European Commission.
commentaries to the regulation and they were waiting for the regulation to be passed to publish them. They would simply add corrections regarding provisions changed at the very last moment, then put out commentaries including their critical opinions.

Let me recall a story from early 1990s from my homeland. The story of one of the professors from Poland, who – as a new minister at this time – was one of the founding fathers of the new law regulating the stock exchange market enacted in Poland after the fall of communism. He had to draft the new law from scratch, as there was no stock exchange market in this part of Europe before 1989. He had to create something which would work in the Polish circumstances. He prepared a draft of the new law and sent it to all the professors he knew who may have had something to say about the subject, and simply asked them for comments. He never received any. The draft law underwent the typical legislative process and once the law was passed, suddenly all these professors who had received the drafts before, published their critical commentaries. The professor/minister was shocked, not only by the behavior of his friends from academia, but also by the sad fact that all critical commentaries had a point. The professors knew the law would cause problems but simply decided not to publish their opinions during the legislative process, because this left them more space for being critical, being important in the scientific field at the time when the law had already been enacted.

I would therefore like to ask members of the academia to be active when governments and DPAs are in the process of preparing acts which the scientific community may have something to say about. This is when we – the data protection authorities and the representatives of the government – actually need this kind of help.

Hence, GIODO joined the consortium preparing the PHAEDRA project which we finalize today. Polish DPA wants to obtain this knowledge as soon as possible. We need the access to studies being done by the academia at the time when we are preparing a regulation – not afterwards. After the law goes into force, the publications may be important to science itself, but rather less important from the practical point of view.

This leads me to the second part of my presentation today, which is the cooperation between data protection authorities, especially those data protection authorities that come from my continent – Europe.

I would now like to recall Jacob Kohnstamm. When I joined the data protection community over four years ago and attended the first meeting of

---

2 Jacob Kohnstamm, Chairman of the Dutch Data Protection Authority, former Chairman of the Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data) gathering all European DPAs, 2010–2014.
the Working Party of Article 29 in 2010, I found the chairman of that Group (Jacob Kohnstamm was the chairman of the Working Party of Article 29 by February 2014) very European-oriented. I do not mean European from the perspective of a European Union institution. The chairman was European-oriented when chairing the meetings, remembering that there are representatives of 27 countries at the time, plus observers, trying to give some European perspective to what is going on and what should be an outcome of the Working Party of Article 29.

Jacob is not a chairman anymore, but he is still a member of the data protection community and works as the Data Protection Commissioner in the Netherlands. There is a saying in Poland, that the point of view depends on where you sit. I am very curious if this saying applies to Jacob. Has his attitude – both personal and that of a member of the national data protection authority – changed when he is not forced to be European-oriented? I hope it has not. Nevertheless, he does not have to be European-oriented anymore and he also needs to deal with the national perspective.

In Mauritius, during the International Conference of the Data Protection Authorities,3 we prepared the declaration regarding the international cooperation in enforcement activities. The last days of discussions concerning the declaration were crucial. There were a lot of deliberations and it turned out that all the participants were looking at the declaration from their own national perspective. Everybody thought about how the new scheme would work in their national procedural environment. That is of course a good approach of a DPA. On the other hand, however, we were preparing a document concerning international cooperation.

The only person who seemed to have adopted the European perspective was the European Data Protection Supervisor, Peter Hustinx.4 He was the one considering the cooperation of different European authorities without being forced to filtrate it down to the national law. The Polish representative of the data protection authority considered the cooperation from the national perspective. So did representatives of Spain, Holland, and so on. Therefore, I would like to call for the adoption of the international perspective. I like the idea of one-stop-shop decisions as common decisions of all data protection authorities – members of the European Data Protection Board.

Thinking about EDPB and the consensus or unanimity in its decisions, I would like to deliver the final message. Being a scientist and loving the history,

3 International Conference of Data Protection and Privacy Commissioners is the biggest, annual data protection event that takes place for regular basis, which brings together not only DPAs all around the world but also industry representatives and academics having expertise in data protection issues.

I would like to recall Poland in the 17th and 18th century. This is when *liberum veto* – a specific parliamentary device – was applied. It is a system of unanimous voting. *Liberum veto* meant that at the sitting of the Diet (Sejm) of the Republic of Nobles, any person who opposed the draft law could say: “I’m against” – *Liberum veto*, the free veto. This ended the discussion. For a long time this device existed only in theory, and was not used. As long as it was not used, the country was quite prosperous. However, when *liberum veto* started to be applied, Poland went to ruin and lost its independence in the end of the 18th century. This is because *liberum veto* was used to kill all improvements. The Diet was unable to make decisions, because all its members considered solely their own position.

The proposal for a General Data Protection Regulation explicitly provides for international cooperation mechanisms for the protection of personal data between DPAs.\(^5\) It is significant that the cooperation between DPAs will no longer be just one of the possible options, but a rule arising from the new EU law. However, we still have to be prudent in developing new legal principles of cooperation and coordination between DPAs, having in mind their different national interests or legal obstacles to practical cooperation between them. Regardless of the importance and necessity (both for DPAs themselves and the market) of the common decision-making mechanism or other forms of coordinating the activities, this mechanism has to take into account all divergences and other circumstances, which may hamper the developed forms of cooperation.

Hence, various researches and analyses – such as the one conducted within the PHAEDRA project – are all the more important, because they constitute a stage of conceptual work on the effective models of cooperation between DPAs. They are to ensure that the implemented mechanisms in the form of specific provisions of the new law on personal data protection in Europe can become an effective tool in the hands of DPAs for the realisation of an idea of truly harmonized privacy protection law in Europe.

Therefore, any expert’s opinion coming from the academic society – so experienced in analyzing the mechanisms functioning in other fields, such as competition protection or telecommunications sector – is an invaluable help for the development of mechanisms of practical and helpful cooperation between data protection authorities.

---

Introduction

Paul De Hert*, Dariusz Kloza*, Paweł Makowski**

** Biuro Generalnego Inspektora Ochrony Danych Osobowych

1. It will be a truism to state that globalisation and recent rapid development of information and communications technologies have resulted in increased trans-border personal data transfers and – at the same time – in the elevation of corresponding risks.¹ This phenomenon both has placed the governance of privacy and personal data protection at the international level and has made data privacy violations with cross-border implications much more frequent. As a result, there grew a critical need for stronger, more enhanced and more efficient cross-border cooperation between relevant supervisory authorities, i.e. between those public bodies that are tasked with “the day-to-day protection of data privacy”, on whose shoulders “lies the main burden of effective protection”?²

The status quo of such cooperation leaves much to be desired. Nowadays – to ensure an appropriate level of protection of privacy and personal data and to investigate and prosecute violations, should they occur – these supervisory authorities face constraints by way of human and/or budgetary shortages, practical, institutional and legislative set-ups and similar factors. Often, due to the lack of cooperation and coordination, these resource-constrained authorities may also investigate the same privacy issue, which is, in effect, a duplication of effort.

For these reasons, policy-makers, authorities themselves and academics – since as early as 2000s – became preoccupied with diagnosing the problem

² D. Kloza and A. Galetta, Towards efficient cooperation between supervisory authorities in the area of data privacy law, in this volume.
and with the quest for solutions. This is particularly acute with the pending reform process of the European Union (EU) data protection framework, where the proposed regulation would make cooperation a legally binding obligation and would set forth the conditions and procedures therefor. In that regard, the reform pays the biggest attention to the one-stop-shop mechanism, designed to work within the borders of the EU and to facilitate and simplify the enforcement process for all actors involved: supervisory authorities, data controllers, data processors and – especially – data subjects.

The PHAEDRA research project, or “Improving Practical and Helpful cooperation between Data Protection Authorities” (2013–2015), co-funded by the EU under its Fundamental Right and Citizenship Programme, has been aimed precisely to contribute to this debate. Its principal objective – realised by a consortium comprising four institutional partners from Belgium, the United Kingdom, Spain and Poland – was, therefore, to help improving practical cooperation and coordination between data protection authorities (DPAs), privacy commissioners (PCs) and privacy enforcement authorities (PEAs). Having recognized the critical need for more efficient international cooperation of these supervisory authorities, the two-year research analysed the state-of-the-art thereof, interacted with these authorities (via, among others, interviews, surveys and workshops) with a view how to improve their practical cooperation and – finally – advised policy-makers and supervisory authorities themselves in that regard, in parallel raising awareness about the problem at stake. The results of the project strengthen the belief of the consortium that its work has achieved notable successes.

2. This book is composed of selected interventions made at the final conference of the PHAEDRA project, held on 12 December 2014 in Kraków, Poland. These contributions are preceded by invited comments written by the experts in the field. Each of these papers – in one way or another touching upon various aspects of cooperation between supervisory authorities – contributes to the unambiguous conclusion that the efficiency of such cooperation is an essential element of the effective protection of the fundamental rights to privacy and personal data protection.

The book is opened by a letter of Dr Edyta Bielak-Jomaa, Inspector General for Personal Data Protection of Poland and by a foreword of Dr Wojciech R. Wiewiórowski, Assistant European Data Protection Supervisor and former Inspector General of Poland, discussing expectations and solutions for reinforced European and international cooperation. We thank them both for their interventions.

---

The various contributions to the present volume are split into two parts, the first gathering invited comments. In the first chapter, Blair Stewart, Assistant Commissioner in the Office of the Privacy Commissioner of New Zealand, building on PHAEDRA final results, provides a few further recommendations for helpful and practical cooperation from the global perspective. David Wright and Kush Wadhwa – representing one the PHAEDRA partners – Trilateral Research & Consulting LLP – report in the second chapter how supervisory authorities themselves view cooperation and coordination and what barriers thereto they have identified. Two subsequent chapters were written in Brussels, at the premises of Vrije Universiteit Brussel, coordinator of the PHAEDRA project. Paul De Hert and Auke Willems deal with the challenges posed by overlapping jurisdictions and requests for mutual legal assistance to fundamental rights. Finally, Dariusz Kloza and Antonella Galietta offer twenty-three recommendations towards the efficiency of cooperation between supervisory authorities.

The second part comprises selected interventions from the final conference of the PHAEDRA project. Endre Győző Szabó of Hungarian DPA highlights the Weltimmo case, especially the question of jurisdiction and applicable law, in light of the future EU one-stop-shop regime. Marek Múčka of Slovak DPA advocates for a unified approach towards the legal qualification of biometric data. Dimitar Gjeorgievski of Macedonian DPA, having discussed their own experience of international cooperation, suggests the establishment of a regional secretariat for “South East” DPAs to foster “development and integration of data protection and privacy principles in the region”.

In a similar vein, Lahoussine Aniss of Moroccan DPA, argues for a more robust exchange of expertise between “mature” and “new” supervisory authorities. All the authors to this collection of papers have done an excellent and outstanding job and deserve our applause.

3. At the end, we wish to draw the attention of the reader to the fact that the PHAEDRA project turned out to be only the beginning of more comprehensive work on the question of cooperation of supervisory authorities. Recognizing the need arising from the reform of the EU data protection framework, the consortium decided to bid for a follow-up project, PHAEDRA II. Having won, the new project started in January 2015 and focuses on the cooperation of European DPAs (solely), examining in particular the impact of EU data protection reform on the notion of cooperation. The new project tackles three of the biggest challenges facing European DPAs: ensuring


4 D. Gjeorgievski, Institutional experience from international cooperation and joint investigation, in this volume.
consistency, sharing information (including confidential or otherwise privileged information) and practical coordination of enforcement actions.

The reader is kindly invited to stay in touch with the PHAEDRA consortium, especially by consulting the project’s website at http://www.phaedra-project.eu. This website already offers the legacy of the first PHAEDRA project and is meant to become one of the main sources of information on DPAs cooperation.

Warsaw–Brussels, June 2015
Part I

PHAEDRA FINAL CONFERENCE: INVITED COMMENTS
On PHAEDRA’s final recommendations: A few “helpful” tips on how “practical” progress can best be made in enforcement cooperation

Blair Stewart
Assistant Privacy Commissioner, New Zealand

The PHAEDRA Project’s report represents a major milestone in efforts to get to grips with the challenges of cross-border privacy enforcement. The recommendations live up to the opening letters of the project’s acronym as being both ‘Practical’ and ‘Helpful’.

The project has involved expert independent analysis of issues that DPAs and others have struggled with. It has brought together a range of stakeholders in a series of productive workshops exceeding 70 people each and a final conference with over 150. The project has stimulated a lot of interest in the topic and provided a great deal of useful resource through case studies, presentations, findings and recommendations. I have found the case studies an exceptionally useful resource for staff training in cross-border enforcement issues.

This worthy project, financed by the European Commission, is not of course the first to struggle with these issues. As my own country’s privacy laws have OECD (Organization for Economic Cooperation and Development) rather than European origins I am reminded of the detailed discussion recorded in the original report of the Experts Group that developed the 1980 OECD Privacy Guidelines. That report characterised quite similar issues as ‘machinery for cooperation’ and ‘conflicts of laws’.¹

In relation to conflicts of laws the OECD Experts Group contented itself with signalling how difficult the issues were and recommended that ‘countries should work towards their solution’. Their recommendations on

machinery for cooperation were lacking in detail and oriented to a future when the ‘complications associated with [international data networks] become more numerous’. That future is now with us and efforts are being made in various quarters to develop solutions to both the machinery and conflicts of laws issues – or to use the language of the PHAEDRA report ‘enforcement cooperation and coordination’ and ‘standard setting’.

While the OECD signalled the issues more than 3 decades ago, twenty years were to pass before detailed attention was refocused upon them. When it returned to the topic, the OECD published a series of useful studies and adopted a seminal Cross-border Cooperation recommendation in 2007.2

The OECD Cross-border Cooperation Recommendation in turn led to the establishment of the independent Global Privacy Enforcement Network (GPEN).3 The OECD Recommendation was a key factor in shaping APEC’s Cross-border Privacy Enforcement Arrangement (CPEA).4 GPEN and CPEA are two networks that have data protection law enforcement cooperation as their sole focus. The Council of Europe has also done important work in the enforcement cooperation space as has the International Conference of Data Protection and Privacy Commissioners and others.

In the related area of privacy standard setting there have been a host of other bodies involved – Asia-Pacific Economic Cooperation (APEC), Council of Europe (COE), European Union (EU), International Organization for Standardization (ISO), Economic Community of West African States (ECOWAS), Organization of American States (OAS), OECD, World Anti-Doping Agency (WADA) and the United Nations (UN) – to give an incomplete glimpse at the alphabet soup of international bodies that have been active. In relation to creating repositories of enforcement related material – a matter taken up in the PHAEDRA report – they have been several active efforts. GPEN has a sophisticated document repository within its toolbox of cooperation tools. The World Legal Information Institute (WorldLII) has created a huge repository of privacy laws and case reports in its International Privacy Law Library.5

I mention APEC, OECD, GPEN, WorldLII and the others to emphasise that once one moves from a focus on a closed grouping of countries at regional level to explore cross-regional and ultimately global solutions there are a number of other initiatives in play that have potential to work to the benefit of European citizens and consumers.

---

3 https://www.privacyenforcement.net/home.
5 http://www.worldlii.org/int/special/privacy/.
A lot of attention has been paid over several years to internal EU harmonisation and the prospect of integrated cross-border enforcement solutions, for instance, through the proposed GDPR (General Data Protection Regulation) ‘one-stop-shop’. The PHAEDRA report is especially interesting to those of us from outside Europe as it steps away from that inward looking focus to contemplate enforcement cooperation at global level.

The global enforcement scene will benefit from European stakeholders being more engaged beyond the EU borders especially where that engagement does not stop once it crosses the Atlantic but encompasses the rest of the world. The desirable global action on enforcement will benefit from the depth of experience in data protection built up in Europe and from the dedication to protecting what are characterised in Europe as fundamental rights.

However, progress on enforcement cooperation at global level – or even between the EU and individual regional trading blocs – may not necessarily always benefit from the same approaches that suit the European project of ever deeper integration of law and administration. The wider world does not have the tidy starting point of a single data protection standard as does the EU and instead represents a messy mixture of laws of various shapes and sizes, gaps in legal protections and additional quirks, various underlying philosophies (some of which are not based upon any theory of fundamental human rights) and enforcement bodies that do not look like any European DPA. To enforce in the ‘here and now’ Europe must take the world as it is and not as we may wish it to be.

Therefore as an outsider, being neither from Europe nor from a country with an Atlantic coast, I felt the best contribution I could make in this short introduction is to offer a few what I hope are ‘Helpful’ tips on how I think ‘Practical’ progress can best be made in enforcement cooperation. I suggest that the PHAEDRA recommendations be weighed with such considerations in mind:

- **Global enforcement cooperation means cooperating with the locally designated enforcement bodies – these will not always be DPAs.** DPA-only cooperation solutions are only partial solutions as the enforcement of some countries’ privacy laws do not involve DPAs. The PHAEDRA report notes an interesting example of a German DPA entering into arrangements with competition law enforcement bodies – this is the kind of innovative mind-set needed also at global level. The OECD coined the term ‘privacy enforcement authority’ or PEA – terminology also adopted by APEC and GPEN – is an especially useful concept for global cooperation as it focuses on an authority’s function rather than its form or name. It refers simply to a public body that enforces a law having the effect of protecting personal information. This can encompass a DPA, a fair trading or consumer protection body, a competition authority or all manner of other entities so long as they have the core competencies.
• Do not undermine others’ global cooperation mechanisms by building competing structures or by insisting upon using only your own region’s arrangements. The privacy enforcement community is not big enough to have duplicates of everything. Nor will we achieve the goals of global collaboration if we all remain only in our comfortable regional siloes. Sometimes regional arrangements are excellent and worth keeping – in which case authorities could consider opening those regional arrangements to the world. If that is not palatable then authorities should contribute to building, or participate in existing, duplicative global arrangements. Examples of good and not-so-good practice abound in the privacy community and are in many cases documented in the PHAEDRA report. The FTC (US Federal Trade Commission) has long experience in running a successful national/international secure enforcement notification system in the consumer protection area (Consumer Sentinel Network) and at some cost is building a platform on that as the GPEN Alert system. The GPEN online cooperation platform has existed now for years and inexplicably a number of authorities have failed to participate in this sole global online system. Proposals to create new depositories for nonsensitive enforcement (cases, policies, and the like) or alternative enforcement contact directories may undermine existing arrangement – better surely to enhance those existing repositories with supportive European funding, European expertise, translations and enriched content?

• Be practical, incremental, be open to give and take: Do not let the perfect be the enemy of the good. Run before you can walk. (Apologies for the clichés.) Practical progress in enforcement cooperation cannot await agreement to reform the world’s privacy laws. Insisting that the other guy do things your way may not be the best route to cooperation. Interoperability may be a more feasible goal than harmonisation. Focus on the outcome – for instance stopping the bad actor or compensating the victim – rather than trying to tell your cooperation partner how to enforce their own law.

• Be generous: Europe is one of the wealthiest regions on earth, stepping forward to contribute modest amounts of money or time may be all that is required to get some valuable cooperative initiatives off the ground. Sometimes cash is what is needed. Sometimes assistance ‘in kind’ makes a big difference, for instance by opening up training opportunities to out-of-region enforcement staff.

Finally, may commend the European Commission for funding this valuable work and the PHAEDRA consortium for a job well done. The recommendations for action offer a blueprint for further progress towards a more joined up privacy enforcement community.
Cooperation and coordination viewed by supervisory authorities themselves: results of PHAEDRA surveys

David Wright, Kush Wadhwa
Trilateral Research and Consulting

A European consortium has found that most of the world’s data protection authorities and privacy commissioners want to cooperate with each other, but despite good intentions, face various challenges and even barriers to such cooperation. That was one of the principal findings of a project undertaken by a European consortium investigating the extent of cooperation between and among the world’s data protection authorities, especially as a means of leveraging their scarce resources. The two-year project, called PHAEDRA, was co-funded by the European Union, and undertaken by a consortium comprising Vrije Universiteit Brussel (VUB), Trilateral Research (UK), the Universidad Jaume I (Spain) and GIODO, the Polish data protection authority.¹ PHAEDRA is the project’s acronym; it stands for Improving Practical and Helpful cooperation between Data Protection Authorities. The project began in January 2013. Its aim was to help improve cooperation and coordination between data protection authorities (DPAs) and privacy commissioners around the world.

The consortium conducted various activities as part of its investigation, including interviews with DPAs, workshops, roundtables and a conference, desk research and three surveys. The first survey was initiated in February 2013 when the PHAEDRA consortium sent out a questionnaire to 79 data protection authorities and privacy commissioners around the world. The two-page questionnaire had 10 questions asking about areas for improving cooperation and coordination, possible constraints, measures for improving coordination of investigations, sharing information, suggestions for case studies and examples of cooperation. This chapter summarises the results of the survey.

¹ http://www.phaedra-project.eu.
The consortium received 53 responses. The respondents were mainly from European DPAs and privacy commissioners, but also included responses from the Americas, Asia/Pacific, and the Middle East.

In the course of the PHAEDRA project, the consortium conducted three surveys. This chapter summarises the results of these surveys.

I. Results of the first PHAEDRA questionnaire

1. In what areas would you like to see improved cooperation and coordination with other privacy commissioners and data protection authorities (DPAs)?

DPAs were asked to rank five possibilities. Discounting “Other”, the overall ranking from most important to least important is shown in the following charts:

![Figure 1. Importance of factors to improve cooperation and coordination](image)

The list of areas or factors from the questionnaire included:
- Coordination in enforcement actions, especially against multinational data controllers, to avoid duplication of effort and make more efficient use of resources
- Exchange of knowledge, experience and best practice
- Consistency (i.e., avoiding situations where privacy commissioners and DPAs apply different criteria in enforcement actions)
- Measures aimed at converging the powers of privacy commissioners and DPAs
- Other
In evaluating responses, we also looked at the most highly ranked (i.e., given importance of 1 or 2) and the least highly ranked items (given importance of 3, 4 or 5), which revealed that the two most highly ranked areas retained that designation when the rankings were combined, with a slight edge for “Coordination in enforcement actions...”.

Nineteen respondents identified “Exchange of knowledge, experience and best practice”, as the most important factor to improve cooperation and coordination, while 17 identified “Coordination in enforcement”.

Figure 2. Frequency with which each area is ranked as of high importance

Figure 3. Frequency with which each area is ranked as less important
2. What are the chief constraints on you in achieving more cooperation and better coordination?

DPAs were asked to rank five possibilities. Again, discounting *other*, the first possibility below was regarded as the most serious and the last as least serious.

- Lack of information from other privacy commissioners and DPAs about cooperation and coordination activities
- Limited budgetary and/or human resources
- Legal constraints
- Language differences

Figure 4. Frequency with which each constraint is ranked as of high importance

Figure 5. Frequency with which each constraint is ranked as less important
3. At what level would you like to see improved cooperation and coordination? Please tick the relevant ones.

DPAs were offered three choices, in addition to other, i.e., at the regional and international levels and by language group (e.g., Ibero-American group, Francophone group). Most respondents indicated that they would like to see improved coordination and cooperation at either the regional level, the international level or both. In a few cases (10), respondents expressed an interest in improved coordination by language group.

![Figure 6. Levels at which improved cooperation and coordination is desired](image)

4. What measures do you think could be taken to improve cooperation and enhance coordination of investigations with other privacy commissioners and DPAs?

DPAs were given several options to rank in order of importance. Discounting the other option, the first below was regarded as most important, followed in order by the others.

- Online tools to facilitate sharing of information (e.g., intranet)
- Additional resources (manpower, budget)
- A small secretariat for exchange of information and best practice
- An international treaty (i.e., binding instrument)
- A memorandum of understanding or other non-binding instrument
- Amending your enabling legislation
- Regularly scheduled teleconferences to discuss common issues
It is interesting to note that DPAs place greater importance on collaboration than on additional resources, even though many have a shortage of resources for the tasks they perform.

Figure 7. Frequency with which each measure is ranked as of high importance

<table>
<thead>
<tr>
<th>Measure</th>
<th>High Rank</th>
<th>Lesser Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secretariat for exchange of info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online tools to facilitate sharing info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A memorandum of understanding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amending country’s legislation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 8. Frequency with which each measure is ranked a less important

<table>
<thead>
<tr>
<th>Measure</th>
<th>High Rank</th>
<th>Lesser Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secretariat for exchange of info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online tools to facilitate sharing info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A memorandum of understanding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amending country’s legislation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Some measures (e.g., an international treaty or amendment of your enabling legislation) might take a long time. Which measures do you think could be taken in the short term to improve cooperation and coordination?

DPAs made various suggestions. Albania, Bosnia-Herzegovina, Costa Rica, the Czech Republic, Macau, the Isle of Man, Poland, Portugal and Sweden said that the signing of memoranda of cooperation or other non-binding instruments would help foster closer cooperation between privacy commissioners and provide procedures for more effective exchange of information between competent authorities. Hungary agreed with this, but emphasised bilateral and regional agreements. Israel also thought an MoU would be useful, especially for training, educating and exchanging personnel and sharing practical information. Uruguay said it was establishing MoUs with Mexico, Costa Rica and Canada. Poland advocated standardised forms and procedures.

Portugal had some specific suggestions regarding an MoU. It said its implementation could be better and more easily achieved through the establishment of a common information platform (internal website), where key information should be available, such as a list of contact persons; a resumé of the powers and functions of each DPA and sectors covered; a repository of guidelines, enforcement actions, best practices and case law (by themes and covering different areas), initiatives aimed at raising awareness; a discussion forum where any DPA may request assistance or advice; where they can discuss "hot" topics informally; where they can share news and experience, where they can find a calendar of major international activities; and where they can collaborate on joint actions. Portugal felt that some mechanism was needed to push DPAs to participate regularly. It said some basic rules might be needed, for example, regarding deadlines to reply to each other, otherwise cooperation won't be effective. Serbia and Vietnam also mentioned online tools to facilitate sharing of information (e.g., an intranet).

Australia said the OECD Global Privacy Enforcement Network has already developed a website to share information, and is in the process of developing a non-binding instrument to facilitate coordination and cooperation. The Asia Pacific Privacy Authorities (APPA) is another network established to facilitate exchange of information between DPAs. The GPEN would seem to address Hong Kong's perceived need for online and informal sharing of views, enforcement actions being taken and/or experience sharing in a secured environment.

\[^2\text{http://www.privacyenforcement.net/}.\]
\[^3\text{http://www.appaforum.org/}.\]
France said it believes that the International Conference is the most appropriate basis on which cooperation should be built. However, it recognises that the GPEN offers a privileged opportunity for the exchange of good practice and that it is a useful forum and an efficient tool for cooperation. It felt consideration should be given to the possibility that the GPEN be involved and participate in the work of the International Conference (e.g., by creating windows of cooperation).

Bavaria and Finland saw need for clear agreements, especially about who is the leading institution in an enforcement action. Bavaria suggested the creation of an online portal for an exchange of views. It also saw a need for a repository of data protection acts, translated into at least English. Estonia was of a similar mind regarding a website operated by a small secretariat that could initiate questionnaire and topics. Cyprus, Ireland, the Isle of Man, Ontario, Macedonia, Moldova, Russia and Switzerland also supported an Intranet for DPAs, teleconferencing and a small secretariat. Estonia referred to CIRCA\textsuperscript{4} for uploading documents, but said there is a lack of an interactive environment for the exchange of comments and questions.

Bulgaria saw a need for a framework document containing common rules for information exchange and cooperation on joint inspections.

Canada and Belgium saw a need for an efficient, secure mechanism for authorities to indicate that they are interested in an issue or incident, determine whether other authorities are interested in working together on a particular issue and forming a group to pursue the matter. Canada and New Zealand said authorities should consider making greater use of GPEN, although the functionality of the website needs to be improved. Also needed is a discussion of how GPEN relates to other initiatives, such as the working group to promote international enforcement coordination, created at the Mexico City International Conference in 2011. Canada said authorities need to assess their ability to cooperate and share information and, where necessary, discuss this with their governments. New Zealand said countries could refer to the OECD Recommendation on Enforcement Cooperation as a blueprint for updating their data protection laws. The Slovak Republic also said DPAs should work toward a legally binding instrument for privacy coordination.

\textsuperscript{4}CIRCA: Communication and Information Resource Centre Administrator, is a simple groupware, developed by the European Commission under the IDA Programme. It is a web-based application providing online services that offer a common virtual space for Workgroups, enabling the effective and secure sharing of resources and documents. Its architecture is based on Open Source Software. It has been widely used by the EU public administrations since 1996. It is also a generic service (including help desk, assistance and training services) operated by the European Commission’s Directorate-General for Informatics (DIGIT) to support the work of the numerous EU committees. For more information see: http://ec.europa.eu/idabc/en/document/6540.html.
Belgium, Colombia, Germany and Japan saw a need for information sharing on major cross-border cases/issues, including legal assessments and envisaged measures; sharing of best practices; joint case studies; regular meetings, workshops and conferences on defined cases and issues with high relevance for data protection in an international context. Liechtenstein also saw a need for regional meetings of German-speaking countries. The Slovak Republic also said cooperation could start at the neighbour level.

France suggested the creation of a task force dedicated to enforcement with regular meetings in order to exchange about best practices, on-going cases or technical aspects.

Greece suggested each DPA should appoint at least one contact person who would be responsible for coordination of all activities between the DPAs.

Iceland saw a need for regular inter-European meetings but commented that it could not attend such meetings due its severe lack of funding. Italy, Lithuania, Serbia, the Slovak Republic and Sweden also mentioned a need for additional resources.

Israel suggested developing a model proactive regulatory approach towards data protection and combining legal and technological R&D activities, somewhat like the Article 29 Working Party, but able to undertake a wider range of activities.

Japan felt that non-binding instruments like the APEC Cross-Border Privacy Enforcement Agreement were helpful for improving the international framework of cooperation.

Mexico, Montenegro and Ontario had several suggestions for improving short-term cooperation and coordination, but all in line with other DPAs. Mexico mentioned:

- Establishing cooperation agreements between authorities to coordinate enforcement actions;
- Sharing information on criteria, studies, guidelines, resolutions and relevant case cross or common materials that could serve as a reference to other authorities;
- Creating a website that would serve as a kind of library, in which the authorities could find different types of documents (resolutions, criteria, guidelines, regulation) on various topics of interest;
- Creating working groups with well-defined objectives that provide continuity for specific cooperation projects;
- Developing forums and conferences focused on regional, international or group issues;
- Providing training and professional practices to the personnel of other data protection authorities. Moldova also supported joint workshops and study visits in order to share experiences and best practices. Ukraine cited a need for some training and an expert from some other DPA to help them. Belgium also suggested creation of a program
between DPAs that could help in the exchange of experiences and best practices with regard to, for example, binding corporate rules (BCRs), privacy impact assessments, inspections and internal organisation of work. Vietnam said that trainers should have (of course) good skills, good communication and a sensitivity towards international cultures.

Netherlands said that, in the absence of enabling legislation, DPAs could overcome coordination difficulties by identifying and recognising the differences in their legal frameworks and trying to find work-arounds, or to limit their cooperation to those areas where cooperation is feasible. This could already be done on the basis of a bilateral MoU. The US was of a somewhat similar view: It felt that adoption of an online enforcement coordination tool, and informal arrangements with other authorities to cooperate on appropriate matters using existing authority, are the most promising short-term measures.

In the short term, the UK said all privacy enforcement authorities should sign up to an international enforcement coordination mechanism which would allow for (a) sharing of best practice and information exchange for both public and private, national and regional activity and (b) pooling intelligence about past cases involving data controllers not established in the context of the processing in the privacy enforcement authority’s jurisdiction. It should allow for knowing where a data controller is established and identify the relevant authority for taking this forward. It should also allow for PEAs to signal that they are interested in the particular issue because they have legal authority regarding the data controller or because they have a complaint about the data controller from their citizens. This would allow other PEAs and the lead DPA to coordinate action as appropriate.

Vietnam said that establishing a higher level of trust and sustaining relationships between DPAs so that they are willing to share information would help improve cooperation and coordination in the short term.

6. If you were to undertake an enforcement action against a data controller suspected of non-compliance with data protection or privacy legislation in your jurisdiction and where the case has cross-border dimensions, would you be able to share information, including confidential information, with other privacy commissioners and DPAs?

Although DPAs have frequently mentioned the difficulties in sharing information, especially confidential information, as a potential barrier to improved coordination enforcement actions internationally, in their responses to this question, it seems that most privacy commissioners and data protection authorities are able to share information with their counterparts in
other countries, as depicted in the figure below. However, in many instances, whether DPAs are able to share confidential information is either context-dependent (the possibility of sharing information depends on the particular situation) or comes with conditions or there are no provisions in their relevant legislation dealing with such matters.

![Diagram: Ability of DPAs to share information across borders]

Figure 9. Ability of DPAs to share information across borders

7. How many full-time employees does your organisation have? Of those, how many work on international relations, either full-time or for a significant part of their time? Does your organisation have a unit or department dedicated to international relations?

The responses to this question are summarised in the following table:

<table>
<thead>
<tr>
<th>Data Protection Authority</th>
<th>Number of employees</th>
<th>Number dedicated to international relations</th>
<th>Does the DPA have a unit dedicated to international relations?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albania</td>
<td>29</td>
<td>6</td>
<td>Y</td>
</tr>
<tr>
<td>Australia</td>
<td>62</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>Austria</td>
<td></td>
<td>1.5</td>
<td>N</td>
</tr>
<tr>
<td>Bavaria</td>
<td>16</td>
<td>1</td>
<td>Y</td>
</tr>
<tr>
<td>Belgium</td>
<td>50</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>Berlin</td>
<td>37</td>
<td>2</td>
<td>Y</td>
</tr>
<tr>
<td>Data Protection Authority</td>
<td>Number of employees</td>
<td>Number dedicated to international relations</td>
<td>Does the DPA have a unit dedicated to international relations?</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Bosnia &amp; Herzegovina</td>
<td>24</td>
<td>3</td>
<td>Y</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>73</td>
<td>4</td>
<td>Y</td>
</tr>
<tr>
<td>Canada</td>
<td>170</td>
<td>6</td>
<td>N</td>
</tr>
<tr>
<td>Colombia</td>
<td>20</td>
<td>3 part-time</td>
<td>Y</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>1 [28]³</td>
<td>[3]</td>
<td>[Y]</td>
</tr>
<tr>
<td>Cyprus</td>
<td>14</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Czech Rep</td>
<td>100</td>
<td>1 + 4 part-time</td>
<td>Y</td>
</tr>
<tr>
<td>Denmark</td>
<td>32</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>Estonia</td>
<td>18</td>
<td>5 (0.5FTE)</td>
<td>N</td>
</tr>
<tr>
<td>Finland</td>
<td>20</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>France</td>
<td>171</td>
<td>7</td>
<td>Y</td>
</tr>
<tr>
<td>Germany</td>
<td>80</td>
<td>7</td>
<td>Y</td>
</tr>
<tr>
<td>Greece</td>
<td>39</td>
<td>7 (1 FTE)⁶</td>
<td>N</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>76</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>Hungary</td>
<td>59</td>
<td>5</td>
<td>Y</td>
</tr>
<tr>
<td>Iceland</td>
<td>4</td>
<td>4</td>
<td>N</td>
</tr>
<tr>
<td>Ireland</td>
<td>26.5</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>Isle of Man</td>
<td>4</td>
<td>0</td>
<td>N</td>
</tr>
<tr>
<td>Israel</td>
<td>25</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>Italy</td>
<td>109</td>
<td>4</td>
<td>Y</td>
</tr>
<tr>
<td>Japan⁷</td>
<td>2 – 13</td>
<td>0 – 4</td>
<td>Y</td>
</tr>
</tbody>
</table>

³ The Costa Rican authority said it was soon to begin a major recruitment, which would result in staff numbers as indicated in the square brackets.

⁶ Seven staff work on international relations, but their total time is equivalent to one full-time employee (FTE).

⁷ The Japanese Ministry of Economy, Trade and Industry (METI) responded to the questionnaire. However, in doing so, it noted that, in Japan, there is no authority dedicated to data protection. Each ministry enforces privacy in its own jurisdiction, and each ministry and external agency has a unit working on data protection. METI’s response to the questionnaire joined answers from various ministries and agencies. With regard to FTEs, it said there are cases where some departments or units also cooperate on privacy issues. The number of employees within a ministry/agency working on international relations on privacy and data protection ranged between 0 and 4. While it has a department or unit dedicated to international relations, data protection was only a part of its function.
<table>
<thead>
<tr>
<th>Data Protection Authority</th>
<th>Number of employees</th>
<th>Number dedicated to international relations</th>
<th>Does the DPA have a unit dedicated to international relations?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Korea</td>
<td>40</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>2</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>Lithuania</td>
<td>30</td>
<td>3</td>
<td>Y</td>
</tr>
<tr>
<td>Macau</td>
<td>31</td>
<td>2</td>
<td>N</td>
</tr>
<tr>
<td>Macedonia</td>
<td>26</td>
<td>1</td>
<td>Y</td>
</tr>
<tr>
<td>Mexico</td>
<td>87</td>
<td>11 part-time</td>
<td>Y</td>
</tr>
<tr>
<td>Moldova</td>
<td>18</td>
<td>3</td>
<td>Y</td>
</tr>
<tr>
<td>Montenegro</td>
<td>15</td>
<td>2</td>
<td>N</td>
</tr>
<tr>
<td>Netherlands</td>
<td>80</td>
<td>7</td>
<td>Y</td>
</tr>
<tr>
<td>New Zealand</td>
<td>30</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>Ontario</td>
<td>100</td>
<td>9</td>
<td>N</td>
</tr>
<tr>
<td>Poland</td>
<td>130</td>
<td>8</td>
<td>Y</td>
</tr>
<tr>
<td>Portugal</td>
<td>26</td>
<td>1</td>
<td>Y</td>
</tr>
<tr>
<td>Russia</td>
<td>298</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>Serbia</td>
<td>43</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Singapore*</td>
<td>40</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>164</td>
<td>2 (+5)</td>
<td>Y</td>
</tr>
<tr>
<td>Slovak Republic</td>
<td>28</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>Slovenia</td>
<td>33</td>
<td>4</td>
<td>N</td>
</tr>
<tr>
<td>Sweden</td>
<td>40</td>
<td>1 + 4 part-time</td>
<td>Y</td>
</tr>
<tr>
<td>Switzerland</td>
<td>22.7</td>
<td>0.8</td>
<td>N</td>
</tr>
<tr>
<td>Ukraine</td>
<td>43</td>
<td>4</td>
<td>Y</td>
</tr>
<tr>
<td>UK</td>
<td>350</td>
<td>2</td>
<td>Y</td>
</tr>
<tr>
<td>USA (FTC)</td>
<td>45</td>
<td>6</td>
<td>Y</td>
</tr>
<tr>
<td>Uruguay</td>
<td>12</td>
<td>12 part-time</td>
<td>N</td>
</tr>
<tr>
<td>Vietnam</td>
<td>40</td>
<td>2</td>
<td>Y</td>
</tr>
</tbody>
</table>

* Singapore’s Personal Data Protection Commission (PDPC) was formed in January 2013; hence, it is still ramping up its recruitment. It envisages 40–50 employees.
The figures on international relations employees are misleading. Some DPAs have shown the number of all employees fully or partly dedicated to international relations (e.g., Estonian DPA: 5 of 18, but the real full-time-equivalent is around 0.5). Some have shown the full-time equivalent and some have shown only full-time employees (e.g., Denmark: 0 of 32).

We aim to compile a set of case studies, as examples where DPAs or privacy commissioners have investigated the same issue (e.g., Google Street View) and where privacy commissioners and DPAs collaborated or shared the results of their investigation with other privacy commissioners and DPAs (e.g., CNIL shared the results of its investigation into Google’s combining its privacy policies). Could you suggest from your experience any other case studies you think the PHAEDRA consortium could usefully investigate?

DPAs suggested a range of case studies worthy of investigation. The PHAEDRA consortium has carried out 11 case studies, most of which were mentioned by the DPAs in their response to Question 8. Following is a list of the cases mentioned by DPAs. Some of the cases mentioned below are examples of successful cooperation and coordination, others not. Suggested cases marked with an * have been explored as case studies.

Assessment of the implementation of the Data Retention Directive (2006/24/EC)*
- Badoo case (Cyprus DPA cooperated with CNIL and the ICO)\(^9\)
- Big data
- CCTV in public spaces and in the workplace
- Children’s use of the Internet
- Cloud computing
- Consent in the technological age
- Corporate information and advertising
- Data breach at Sony Computer Entertainment Europe Limited*
- Data losses, e.g., a case involving the Isle of Man and the UK ICO
- Data protection implications regarding the research in, and disclosure of, records of the Historic Archive of the National Security Services
- Electronic medical records
- Eurodac
- Europol
- Google’s privacy policy*

\(^9\) Wikipedia says Badoo is a dating-focused social discovery website, founded in 2006 and managed out of its Soho, London headquarters, but owned by a company based in Cyprus, which is ultimately owned by Russian entrepreneur Andrey Andreev. Opinions of Badoo.com on TrustPilot, which are based on user reviews, rather than press releases, rate the site as ‘Very low’.
Google Street View and the collection of WiFi data*
Health data
Heritage information centres and credit risk assets (private and public)
Ibero-American Data Protection Network
Investigations or studies into MNC [multi-national company] data controllers by a single DPA
ISO standardisation
LinkedIn
Methodologies for controllers to fulfil their obligations
Microsoft Services Agreement
Microsoft’s Office 365, which involves cloud services
Nordic Inspection Cooperation
Personal data protection in registers of voters
Powers of tax administration and data protection
Privacy notices
Protection of personal data in public records (land registry, central population register)
Right to be forgotten
Schengen
Self-regulation
Smartphone applications
Social networks (mainly Facebook), notably the investigations by the Irish DPA* and the Nordic countries
Spam (Colombia and Spanish DPAs)
SWIFT case, investigated by the Belgian DPA, results of which were shared with the Article 29 Working Party*
The annual Iberian meetings of Portuguese and Spanish DPAs to share experiences and discuss common issues and cases involving companies with a presence in both countries
The Article 29 WP investigations regarding data retention by health insurance companies and telecom providers
The case-handling workshops under the aegis of the Spring Conference and DPAs’ use of the CIRCA network to exchange information and request assistance for handling similar cases or with the same companies
The investigation of TJX Companies Inc. conducted by the Office of the Privacy Commissioner of Canada and the Information and Privacy Commissioner of Alberta
Unsolicited direct marketing and spammers
Use of biometrics and its relationship with credentials or identity cards
• W3C “Do not track” (standardisation)
• WhatsApp*
• Google Glass*
• Bilateral cases regarding websites/services operating in one country and processing data related to subjects from another country.

8. Could you also provide some other examples involving cooperation (e.g., training) between your organisation and one or more other privacy commissioners and DPAs?

Albania mentioned the training of its personnel that it had received from other DPAs. It has also undertaken some study visits to more developed European authorities.

As an example of cooperation, Australia cited the fact that the Asia Pacific Privacy Authorities (APPA) has established a Technology Working Group made up of representatives from each APPA member organisation. The Group collaborates on common issues experienced across APPA jurisdictions such as the changes to Google’s privacy policy. APPA has also established a Communications Working Group made up of communications professionals from each APPA member organisation, who consult on com-
communications matters. The Group’s principal activity is collaborating on Privacy Awareness Week.10 Other examples of successful cooperation include the Asia Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement (CPEA)11 and the GPEN.12

Austria said one of its employees underwent a training of two months at CNIL, while another spent several weeks at the Swedish DPA. The Austrian DPA contributed to several data protection-related twinning projects and cooperated closely with the concerned DPAs (Montenegro, Lithuania, Latvia, Czech Republic, Malta, Croatia).13

Bavaria cited examples of cooperation and coordination among the German DPAs in regard to Google-Analytics, analysis of apps, regular meetings on special themes. It cited examples between European DPAs such as exchange about questions of international data processing, i.e., standard contractual clauses and binding corporate rules.

The Berlin DPA also mentioned Google Analytics, as an issue intensively discussed at the national level. This resulted in concessions by Google (limited to Germany). Furthermore, since 1980, the Berlin Commissioner for Data Protection has been convening the International Working Group on Data Protection in Telecommunications, which has provided a platform for exchanging information on these issues and which has adopted numerous common positions, working papers and memoranda.14

The Bosnia and Herzegovina DPA has benefitted from “Twinning Assistance to the Personal Data Protection Agency” in cooperation with the Data Protection Commissioner of Saxony (Germany). The purpose of this project was to strengthen the protection of personal data processed by public authorities and law enforcement agencies in accordance with European standards. The project was successfully completed on 31 March 2010.

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. Canada was one of the founding members of the Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP),

10 http://www.privacyawarenessweek.org/.
12 http://www.privacyenforcement.net.
13 Word cloud created utilising tool at Wordle.net.
14 These can be found at http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdt.
which has an important capacity-building component. The Canadian OPC has had several short-term (of four or five weeks duration) staff exchanges with the CNIL, the FTC, the ICO and Mexico’s IFAI.

As an example of good cooperation, the Czech Republic mentioned the TAIEX seminars and study visits held in cooperation with DPAs from different countries, mostly from the Central and Eastern Europe region.16

Denmark said the Nordic countries have a tradition of meetings and sharing experiences and, some years ago, training. They also undertake joint supervisory actions on a case-by-case basis. Finland also mentioned Nordic cooperation in meeting with expert lawyers and media officers. Iceland mentioned the Nordic countries’ having an exchange program for DPA employees, although it had not used that program.

The Baltic DPAs (Estonia, Latvia and Lithuania) meet regularly. They have cooperated regionally on two joint supervisions, one of which was of the Radisson Blu hotels. They also cooperate on monitoring and issuing recommendations.

The Federal Commissioner of Germany said it is a member of and cooperates with the following bodies:

- International Conference of Data Protection and Privacy Commissioners
- International Working Group on Coordination of Privacy Enforcement
- International Working Group on Data Protection in Telecommunications (“Berlin Group”)
- OECD Working Party on Information Security and Privacy (WPISP)
- Global Privacy Enforcement Network (GPEN)
- Accountability Project
- Council of Europe T-PD (Convention 108)
- Coordinated Data Protection Supervision Group of Eurodac
- Coordinated Data Protection Supervision Group of the European Visa Information System (VIS)
- Joint Supervisory Board of Europol
- Joint Supervisory Authority of the Schengen Information System (SIS I; in near future SIS II)

15 http://www.afapdp.org/.
- Joint Supervisory Authority of the European Customs Information System
- European Conference of Data Protection Commissioners (“Spring Conference”)
- Case-Handling Workshop.

In addition, it has a bilateral cooperation arrangement with the Privacy Commissioner of Canada. It has also cooperated with other DPAs on a case-by-case basis, inter alia with the DPAs of Bulgaria, Macedonia and Moldova.

Japan has cooperated with other privacy commissioners and DPAs in a case involving the leakage of personal data, but did not provide further details. For its part, Macao said it cooperated with some other DPAs, by contacting a designated contact person in GPEN. It raised formal requests of assistance and, on one occasion, technical support to find out the physical location of a website server. It sent staff to Hong Kong to attend training courses organized by the Office of the Privacy Commissioner for Personal Data.

The Polish DPA (GIODO) also mentioned most of those bodies listed above, as well as the Central and Eastern Europe Data Protection Authorities Group. GIOD0 said it was also participating in some international projects: the Leonardo Da Vinci (LDV) mobility projects, LDV partnership projects, study visits and twinning projects.17

Greece and Hungary also mentioned the Case Handling Workshop as an example of cooperation as well as twinning projects.

Hong Kong gave as examples the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), the Data Privacy Subgroup of the APEC Electronic Commerce Steering Group, the Asia Pacific Privacy Authorities (APPA) and the Technology Working Group (TWG) of APPA, which Hong Kong convenes. The TWG has carried cooperation including the enquiry into Google's privacy policy change, sharing of views on cloud computing for the purpose of publishing guidelines for industry, and other exchanges of information on technology developments that might impact personal data protection.

Several countries, including Hungary and Ireland, mentioned the TAIEX study visits. Ireland said it had hosted other DPAs at its office and gave one DPA inspection powers under its Act in the conduct of an audit.

The Isle of Man mentioned regular informal communication and exchange of views between its Office, the UK, Ireland, Jersey, Guernsey and Gibraltar.

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”.

The Italian DPA gave as an example of cooperation its membership in the EU privacy taskforce, led by CNIL, which investigated Google’s privacy policy changes and the relevant consequences for users. It also mentioned GPEN of which it has been a member since 2010. It has also participated in several twinning and TAIEX projects (involving the DPAs and/or competent institutions from Croatia, Turkey, Albania, former Yugoslav Republic of Macedonia, etc.), providing know-how and experience in implementing their data protection legislation.

Mexico cited as an example of cooperation the trainings provided by senior officials from the Canadian Privacy Commissioner’s Office and the US Federal Trade Commission. Mexico noted that it is already part of the system APEC Cross Border Privacy Rules (CBPRs), holds the presidency of the Ibero-American Data Protection Network and is an active member of the APPA. Mexico has also collaborated bilaterally with CNIL regarding the Airline Advance Passenger Information System (APIS), particularly with regard to the legal basis for international data transfers between Mexico and France.

Montenegro gave examples of a Twinning project “Implementation of Personal Data Protection Strategy” and study visits to Austria, Germany and Slovenia.

The Dutch and Canadian privacy enforcement authorities jointly carried out an investigation into the handling of personal information by WhatsApp Inc., a California-based mobile app developer.18

Vietnam said its opportunities to cooperate with others have been somewhat limited. It does, however, attend the International Conference as well as other conferences and events within APEC.

9. Do you have any other comments or suggestions regarding legal, technical and/or political factors that could help improve cooperation or that act as barriers to cooperation?

The following is a selection of the responses received. The Office of the Australian Information Commissioner (OAIC) said that enforcement in the online environment continues to be a challenge, particularly in relation to jurisdiction issues. The OAIC would welcome the sharing between DPAs of legal reasoning relating to how DPAs establish jurisdiction in matters relating to global data flows.

---

18 For more information about the joint investigation, see http://www.dutchdpa.nl/Pages/en_pb_20130128-whatsapp.aspx.
Belgium said that an Internet platform, such as a discussion forum accessible to all DPAs, could be organised to help DPA to communicate easily, receive responses quickly and to access information in an organised manner.

The Office of the Privacy Commissioner of Canada (OPC) said that, in its view, the most important priority is working together on enforcement and compliance issues and that it is valuable to share information on government initiatives. “Once we have a clearer idea of what we are trying to achieve, we need to develop a plan or strategy to achieve this”, said the Canadian respondent. “Identifying collective issues or priorities would be valuable, recognizing that events may require flexibility”.

Cyprus said the issue of international cooperation with third countries should be given thorough consideration in the frame of the discussions about the proposed DP Regulation.

The Finnish DPA suggested creation of a legal database where each data protection authority could share decisions with others. The legal database would help avoid divergent decisions about the same matter.

CNIL said that data protection authorities should have a view of the forensic tools used by other DPAs in order to have a common technical approach.

The German DPA said that cooperation and information-sharing between DPAs should focus on cross-border cases of high relevance for data protection in an international context, i.e., cases where data subjects at an international level are affected or cases concerning international transfers between private or public bodies. Common technical and language standards are important. A good example of a body performing effective information sharing is the secretariat of the Article 29 Working Party. Effective information sharing and cooperation should not result in additional transfers of huge amounts of data.

Greece said that factors that would help improve cooperation include these:

- more human resources
- online tools
- an instrument to facilitate the exchange of information
- a coordinator or coordination body.

The Hungarian DPA said that short-term study visits and seminars were useful to gain first-hand experience and knowledge from other colleagues.

The Icelandic DPA is facing severe budget cuts, which will affect the work of the Authority. The number of cases grows every year and, at the same time, the cases are becoming bigger and more complicated.

IILITA, the Israeli DPA, said the connection between the data protection authorities and other policy-making fora, such as the WTO and UNCITRAL, should 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 Article 29 Working Party. The interaction between data protection, information security and cyber-security may have the potential for ripe data protection concepts to break new ground.

Garante, the Italian DPA, said there should be a specific provision in the law to facilitate a fruitful exchange of information among DPAs without breaching confidentiality rules, which should also make up the legal basis for enforcing procedures or measures initiated by other DPAs. The issues of jurisdiction and applicable law should also be addressed and clarified. In the light of the new cooperation and consistency mechanism pursuant to Article 55 and other Articles in chapter VII of the proposed EU General Data Protection Regulation, there will be an increase of the activities at EU level. This is why the Italian DPA considers it necessary to introduce a European funding mechanism to enable the DPAs to fulfill the aforementioned obligations to cooperate.

The Liechtenstein DPA said it has participated several times in the Case-Handling Workshops, which have been useful. However, these are held less frequently now due to budgetary cuts. Small secretariats seem to be necessary for the organisation of exchanges of views.

The Mexican DPA said one of the main barriers is the lack of regulation and an authority guarantor of the right to protection of personal data with sufficient powers to enforce the regulations that exist to regulate this right, as well as the principles and criteria relevant to this right. It is essential to develop tools and mechanisms to harmonise the various regulations and establish minimum standards for the treatment of personal data internationally.

The Dutch DPA cited the collaboration between the Dutch and Canadian authorities and their having made the best use of each other’s expertise in their joint WhatsApp investigation.

The Office of the Privacy Commissioner (OPC) of Canada said that generally there could be better coordination among DPAs, which may yield better outcomes for consumers and leverage use of limited DPA technical resources. Sometimes political or philosophical differences get in the way of global cooperation, but there are large areas of commonality. It would be helpful if the PHAEDRA project could address this issue. The project could also consider the need to collectively finance a cooperative infrastructure (e.g., a small secretariat). 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. Insightful suggestions from expert outsiders as to what might work would be welcomed.
The Ontario DPA noted that, in 2010, data protection authorities and privacy commissioners from around the world unanimously adopted a resolution in which privacy by design was cited as an essential component of privacy protection. Recently, jurisdictions such as the U.S. and EU have introduced privacy by design into proposed data protection regulation and policies. If data protection authorities and privacy commissioners continue to incorporate privacy by design into their respective laws, cooperation on investigations and enforcements will be advanced and organisations will avoid privacy harms, as opposed to offering systems of redress after the breaches have occurred.

Poland said that cooperation is composed of three elements: the expertise and availability of the DPA, the possibility of cooperation and its actual application. One of the solutions for an improvement of the actual cooperation in the short-term would be a non-binding instrument in order to reach common understanding of the procedures for cooperation (forms, language, time limits, expected activities). In the EU, several forms of cooperation (including enforcement actions) have been developed but still most of them are not used by DPAs. The problem is the awareness of the existence of the possible procedure and readiness to follow usually non-binding procedures.

The Portuguese DPA said that international cooperation is an urgent need, as is a consideration of the problems related to applicable law and jurisdiction. As major companies conducting business in Europe are established in the USA, European DPAs face difficulties in enforcement and effectiveness. DPAs have limited powers. At best, DPAs can manage damage control and minimise risks at a later stage. The long-term objective should be to build a worldwide understanding or agreement to tackle privacy problems. While developing short-term strategies to increase effectiveness, consistency and cooperation, DPAs should also invest and develop a binding international framework for the protection of citizens’ privacy rights. DPAs should raise the awareness of stakeholders at the international level to provide an adequate response to the challenges to the individual’s rights presented by the rapid evolution of information technology.

Republic of Macedonia is not yet member state of the European Union, which prevents it from being included in some EU bodies and institutions. It hopes for better cooperation with no borders and limitations.

The Russian DPA said the following could contribute to improving international cooperation in personal data protection:

- development and adoption of unified approaches in order to stop violation of laws concerning personal data, implementation of law enforcement practices appropriate to the purposes;
- establishment of a small secretariat to ensure the coordination of DPA activity in solving issues requiring multilateral engagement;
• creation of a DPA contact list with e-mail addresses for the rapid exchange of information;
• participation in the work of international consultative and advisory bodies;
• broader representation of foreign DPAs in the protection of personal data and the rights of citizens.

DPAs should aim to protect and improve the rights of citizens as personal data subjects and to ensure compliance with the rights to privacy, protection of privacy, personal and family life, regardless of the country of residence.

The Slovak DPA said that DPAs of Member States have many problems, tasks, issues in the rapidly developing environment of IT technology, Internet and electronic tools for monitoring and collection of data. DPAs have budgetary and legal constraints and staff shortages. It is necessary to have clear, stable and binding legislation.

The Swedish DPA said a clear legal basis for international cooperation and joint supervisory measures, including exchange of information, should be part of the EU rules on data protection.

The ICO is open to any mechanisms which are easy to implement, are clear and provide sufficient safeguards when sharing information, including personal data which any privacy enforcement authority (PEA) would have the ability to choose the level of coordination and cooperation suits them.

FTC staff believe that the best way to improve cross-border cooperation is for privacy enforcement authorities to seek opportunities for practical cooperation, even where the ability to cooperate 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 cooperation. FTC investigations are generally non-public and confidential until a case is filed in court or other appropriate circumstances arise. Thus, FTC staff generally can only cooperate with counterpart enforcement authorities willing and legally able to protect the confidential nature of any communications in the course of an ongoing investigation. Also, privacy enforcement authorities without the legal ability to share non-public, confidential information and case-specific evidence with their counterparts across borders should obtain that authority. Promoting enforceable codes of conduct for cross-border data transfers, such as the APEC Cross-Border Privacy Rules, promotes cross-border enforcement cooperation between privacy authorities.

Vietnam views international cooperation as a bridge between VECITA (the Vietnamese authority) and other more experienced authorities around
the world to share information, experiences and skills. It looks forward to having further international cooperation.

II. Results of the second survey questionnaire on support of the PHAEDRA project for DPAs, PCs and PEAs

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 coordination. 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 Cooperation Working Group (IECWG) and identifying barriers to cooperation and ways in which those barriers could be overcome.

III. Results of the third survey questionnaire on investigation and enforcement actions

After the processing of the first and second survey, PHAEDRA conducted a third survey in October 2014. From our survey of DPAs and PCs regarding how they find out about investigation and enforcement actions, we draw the following conclusions:

- 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 ongoing.

• 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.
Dealing with overlapping jurisdictions and requests for mutual legal assistance, while respecting individual rights. What can data protection law learn from cooperation in criminal justice matters?

Paul De Hert, Auke Willems

Introduction

In finding ways to enhance cooperation between Data Protection Authorities (DPAs) it can prove useful to assess the experience of cooperation in other areas of law. In this contribution we examine cooperation in the criminal law area, with the purpose of drawing lessons from this experience. We aim to give a brief overview of some key characteristics of cooperation in the field of criminal law. Two specific areas are of key interest; jurisdictional issues and mutual legal assistance. The primary question this contribution aims to answer is; can DPAs, both European and globally, learn from the criminal justice cooperation experience, in particular the one developed in the European Union, in order to enhance cooperation?

Section 1 will briefly introduce the topic of jurisdiction and the problems that it poses in criminal law. The following sections (2, 3 and 4) will delve deeper into specific rules and mechanisms to handle conflicting claims of jurisdiction. In these sections reference will be made to extradition law, which contains a number of relevant rules on issues of jurisdiction. The second main topic of interest, mutual legal assistance, is examined in more depth in sections 5, 6, 7 and 8. Section 9 will underline some of the problems that have arisen regarding the position of the individual subjected to international cooperation. Sections 10, 11 and 12 then examine platforms for cooperation and coordination that have proven successful in the EU context and will take
a brief look to the future of this area. Finally, section 13 attempts to draw some general conclusions that can prove useful to further cooperation between DPAs.

The topics are presented in a manner highlighting the ‘best elements’ of criminal justice cooperation, selecting those that can be of interest to our aim here and can provide new insights for improving cooperation between DPAs. Note that this study is not merely academic; the two fields, data protection and criminal law, are not completely unfamiliar, as criminal law is being used as a tool for the enforcement of data protection. Although most enforcement takes place via administrative channels, the use of criminal law channels and actors remains a quasi-permanent option. Also note that by no means a complete overview of international criminal justice cooperation is given here, rather a selection of topics that we think can be relevant.

We will look at both international and European mechanisms for cooperation in criminal justice matters, however the focus will mainly be on European and EU cooperation, as this presents an example of an advanced form of cooperation between states.

A. Issues of jurisdiction

1. Jurisdiction: Conflicting claims of jurisdiction

An important question in cooperation in criminal matters (in case of trans-border crime) is how to deal with conflicts of jurisdiction. Conflicts of jurisdiction can be either positive or negative. Positive meaning that two (or more) states claim jurisdiction in a case, negative meaning that no states claims jurisdiction for a(n) (allegedly) committed crime. In both cases coordination is needed, in the former as to what state would be best positioned to deal with the case, in the later the question is how to ensure that the alleged crime does not go unpunished because of a lack of interest to prosecute (which is often a political question). Thus, what state takes the lead in case of a cross-border crime? First, an overview will be given of national rules

---

1 This chapter has thankfully made use of P. De Hert, K. Weis, J. Van Caeneghem and M. Holvoet, *Handboek Internationaal en Europees Strafrecht* (Larcier Uitgevers, 2014).


and principles on which jurisdiction can be claimed, before we will highlight some of the various existing mechanisms that aim to facilitate cooperation between states in dealing with issues of conflicting jurisdiction.5

Conflicting claims (or a lack thereof) of jurisdiction are caused by the very diverse national rules on jurisdiction. Creating expansive territorial or even extraterritorial jurisdiction is not prohibited by international public law and is achieved by states in a variety of ways. It is possible to identify a list of principles or mechanisms used by states to expand jurisdiction beyond their territorial boundaries, and create extraterritorial jurisdiction. A brief overview is given here of the most important principles. Again we note that they do not apply in their entirety in all EU states (let alone all states globally), as national legislation on jurisdiction differs.

The first and foremost principle is that of territoriality; jurisdiction is exercised over crimes committed on a state’s territory (the so called principle of ubiquity). This is the most straightforward and traditional form of exercising jurisdiction.

In addition to territorial jurisdiction, there can also be extraterritorial jurisdiction. This type of jurisdiction can be based on several criteria, such as the nationality of the perpetrator of a crime (active personality principle), the nationality of the victim of a crime (passive personality principle), the type of crime that is committed (protective principle, in case of crimes committed in a foreign country that threaten the security of a state), and the international character of some crimes (universality principle for the most serious crimes). What these all have in common is that a state exercises its criminal jurisdiction over a crime committed (partially) outside its territory.6

Because of the existence of extraterritorial grounds for jurisdiction, but also because of the increasing cross-border nature of crime,7 it is very well possible that two states claim jurisdiction over one (alleged) crime. It is therefore important that clear and objective rules exist as to how to deal with such competing claims, since sovereign states can decide independently when to initiate proceedings against a suspect. Before listing the various mechanisms that aim to facilitate in case of competing claims of jurisdiction, it is important to stress that no such binding mechanism exists at EU level, let alone on a global level. When a positive conflict of jurisdiction appears it is often a political process by which states can use (sometimes binding) guidelines contained in (bilateral) treaties (often these are extradition treaties). One im-

7 In addition to the more traditional cross-border crimes like human trafficking and drug trade, crimes in which it is difficult to establish a locus delicti have grown in importance, like for example cybercrime.
A trans-national double jeopardy rule applies, which prohibits the prosecution of an individual for acts which have already been the subject of a final disposition in another member state. This can lead states to rush proceedings in order to prevent another state from blocking prosecution.

At the other end of the spectrum we find negative conflicts of jurisdiction, which can lead to impunity. This situation is of course especially problematic with regard to alleged perpetrators of serious international crimes. This situation can arise when countries are not willing or capable to prosecute. International initiatives to set up international ad hoc courts (like the Rwanda Tribunal set up by the United Nations) or to set up a permanent court (like the International Criminal Court) can offer relief for certain categories of the most serious crimes. Interesting also is the principle of complementarity in the Rome Treaty on the International Criminal Court (ICC); this court’s jurisdiction is complementary to national criminal jurisdictions, which means that states have the primary responsibility to investigate and prosecute, by doing so to prevent the most serious international crimes. For that reason, the ICC will only step in when national judicial systems fail and it can be demonstrated that states are either unwilling or unable to bring perpetrators to justice. The ICC thus takes a subsidiary position in relation to national courts.

2. Rules on conflicting claims of jurisdiction in extradition treaties

Turning to the ways states ‘arrange’ themselves when confronted with conflicting jurisdiction, one finds some rules in extradition law. Extradition as a form of cooperation is a field of study on its own. Extradition is the formal process by which a state transfers a suspected or convicted person to another state. Extradition is normally regulated by treaties, either bilateral or multilateral. The first multilateral treaty that enabled extradition between European states is the 1957 Council of Europe Convention on Extradition. The treaty entered into force in 1960 and today has been ratified by 50 states, including a number of non-European states (Israel, South-Korea and South Africa). Among EU states the treaty has lost most of its value because of the European Arrest Warrant (EAW), but it is still used in relations with non-EU states in

---

8 See section 9 below.
9 For example the Habré case, see W. Schabas, ‘Senegal’s Chambres africaines extraordinaires to judge Habré’, PhD studies in human rights weblog, 5 February 2013, [http://humanrightsdoctorate.blogspot.co.uk/2013/02/senegals-chambres-africaines.html].
which a EAW cannot be issued. The EAW has within the EU replaced the traditional extradition framework and is based on the principle of mutual recognition; as a result extradition within the EU has become a near-automatic procedure with a limited number of grounds for refusal.\textsuperscript{12}

Extradition does mostly take place on the basis of an extradition treaty. It is often assumed that a pre-existing legal basis is required for a transfer to take place. However, in some instances extradition takes place on an \textit{ad hoc} basis when no treaty is in place. Most European civil law jurisdictions do not allow extradition to take place without a treaty, common law jurisdictions do not per definition exclude this possibility, it however remains rare and the majority of extraditions are treaty based. A set of principles and rules that underpin extradition have formed in the international legal framework that allows for states to retain (partly) their sovereignty when extraditing.\textsuperscript{13}

Most extradition treaties or conventions contain rules or criteria on how to deal with conflicting claims of jurisdiction. A good example of this is the already mentioned European Convention on Extradition,\textsuperscript{14} stating that

‘The requested Party may refuse to extradite a person claimed for an offence which is regarded by its law as having been committed in whole or in part in its territory or in a place treated as its territory’. (Article 7(1) European Convention on Extradition)

This refusal ground is optional (‘may refuse’), therefore it is up to the states to coordinate what state is in a better position to prosecute. Would this ground for refusal have been mandatory, any subsequent test of what state is in the best position to prosecute would have been rendered impossible. Concerning extraterritorial jurisdiction, thus crimes (allegedly) committed outside the territory of the requesting state, the Convention poses that in these situations extradition can only be refused by the requested state:

‘When the offence for which extradition is requested has been committed outside the territory of the requesting Party, extradition may only be refused if the law of the requested Party does not allow prosecution for the same category of offence when committed outside the latter Party’s territory or does not allow extradition for the offence concerned: (Article 7(2) European Convention on Extradition)

\textsuperscript{12} Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States; on the EAW see \textit{e.g.} L. Klimek, \textit{European Arrest Warrant} (Springer, 2014).

\textsuperscript{13} Examples of such rules are the specialty rule and the requirement of double criminality. These will be briefly discussed below in the context of mutual legal assistance where these principles also apply (although not to the same degree). The importance of such principles for DPAs is that these recognise differences between jurisdictions and provide a realistic framework for cooperation, leaving some discretion to states when cooperating.

\textsuperscript{14} \textit{Supra} note 11.
In these cases a sort of ‘double’ jurisdiction is required, a requested state can only refuse extradition when it has a valid claim for jurisdiction.\textsuperscript{15} When this ground applies, the requested state is expected to launch a prosecution itself, if not this would lead to ‘safe havens’ within Europe where criminals could flee and remain unpunished. This is a good example of the so called \textit{aut dedere aut judicare} principle, which refers to the legal obligation of states either to extradite or, in case no extradition is allowed for legal reasons, to prosecute themselves persons who have committed serious international crimes.\textsuperscript{16} The aim is to prevent impunity and ensure that perpetrators of the most serious crimes are being prosecuted.

3. The 2009 EU framework decision on jurisdictional conflicts

The foregoing gave examples of jurisdictional issues being dealt with in the framework of extradition treaties. There is not one single text in international public law that deals in a comprehensive manner with all aspects of jurisdiction. At the level of the Council of Europe, the 1972 European Convention on the Transfer of Proceedings in Criminal Matters\textsuperscript{17} proposed some guidelines to solve positive conflicts of jurisdiction by making it possible to transfer to one state proceedings already begun in another state.\textsuperscript{18} However, the convention was limited in scope and ambition and received only a limited amount of ratifications.

Within the EU, the matter was picked up some decades later, with a 2009 framework decision on how to coordinate conflicting claims of jurisdiction between states.\textsuperscript{19} This framework decision aims to enhance judicial cooperation between EU member states, and to prevent unnecessary parallel criminal proceedings concerning the same facts and the same person.

The text lays out the procedure whereby competent national authorities shall contact each other when they have reasonable grounds to believe that parallel proceedings are being conducted in another EU jurisdiction. It also establishes a framework for these authorities to enter into direct consultations when parallel proceedings exist, in order to find a solution aimed at

\textsuperscript{15} Similar jurisdiction arrangements can be found in other extradition treaties and conventions, for example between the Benelux countries, or those concluded on a bilateral basis between states.

\textsuperscript{16} See C. Bassiouni, \textit{Aut Dedere Aut Judicare: The Duty to Extradite or Prosecute in International Law} (Martinus Nijhoff Publishers, 1995).

\textsuperscript{17} \textit{ETS}, no. 73.

\textsuperscript{18} The convention did not address negative conflicts, since ‘after examination of national legislations it was concluded that situations where no state is competent to act do not arise in member States of the Council of Europe; a regulation of negative conflicts was therefore unnecessary.’ See Explanatory Report, [http://conventions.coe.int/Treaty/EN/Reports/Html/073.htm].

\textsuperscript{19} Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.
avoiding the negative consequences arising from multiple proceedings, or in
the words of the framework decision:

Exchange of information
‘When a competent authority of a Member State has reasonable grounds to
believe that parallel proceedings are being conducted in another Member
State, it shall contact the competent authority of that other Member State to
confirm the existence of such parallel proceedings, with a view to initiating
direct consultations as provided for in Article 10.’ (Article 5(1) framework
decision on jurisdictional conflicts)

‘When submitting a request in accordance with Article 5, the contacting au-
thority shall provide the following information:
a. the contact details of the competent authority;
b. a description of the facts and circumstances that are the subject of the
criminal proceedings concerned;
c. all relevant details about the identity of the suspected or accused person
and about the victims, if applicable;
d. the stage that has been reached in the criminal proceedings; and
e. information about provisional detention or custody of the suspected or
accused person, if applicable.’
(Article 8(1) framework decision on jurisdictional conflicts)
The response by the contacted authority in accordance with Article 6 shall
contain the following information:
a. whether criminal proceedings are being or were conducted in respect of
some or all of the same facts as those which are subject of the criminal
proceedings referred to in the request for information submitted by the
contacting authority, and whether the same persons are involved; in case
of a positive answer under (a):
b. the contact details of the competent authority; and
c. the stage of these proceedings, or, where a final decision has been reached,
the nature of that final decision.’
(Article 9(1) framework decision on jurisdictional conflicts)

Direct consultations (Articles 10–12 framework decision on jurisdictional conflicts)
If parallel proceedings exist, the relevant authorities shall enter into direct
consultations in order to find a solution aimed at avoiding the negative con-
sequences arising from these proceedings. This may lead to concentrating the
proceedings in one jurisdiction. When the relevant authorities enter into di-
rect consultations they must take into consideration all the facts and merits
of the case and all other relevant factors. If no solution is found, the case
shall be referred to Eurojust if appropriate and provided that it falls under its
competence.

The framework decision does not provide for a mandatory termination of
parallel proceedings. On the contrary, it leaves it entirely to the states wheth-
er to concentrate the proceedings in one state (“consultations… which may, where appropriate, lead to the concentration of the criminal proceedings”), or to continue parallel proceedings, creating the danger of imposing a double burden on suspects, as well as rushed proceedings in order to get a decision first. The instrument therefore lacks real ‘bite’ and does not offer a binding solution to conflicts of jurisdiction between EU states. It does however provide some useful guidelines on how to deal with conflicts, which might offer relief to a suspect who is being tried in various jurisdictions.

However, the instrument is silent on the topic of defendants’ rights. These rights are not listed as a specific factor to take into consideration when determining where best to prosecute a suspect. This underlines the instrument’s mostly prosecutorial intentions, as it aims to increase the efficiency in dealing with conflicts of jurisdiction. For those who would have wanted to see a binding EU measure on how to handle conflicts of jurisdiction, the current instrument might be a disappointment. But taking into account the reality that states simply do not want to go this far and lose sovereignty, the current solution might offer the best of both worlds; efficient guidelines, but no loss of sovereignty.

4. The 2013 directive on attacks against information systems

To contrast the modest and non-binding arrangement of conflicts of jurisdiction in the 2009 EU framework decision, we turn to the 2013 directive on attacks against information systems. This directive offers an example of a specific and more developed arrangement of jurisdiction in a specific area of law that naturally triggers competing claims of jurisdiction. The 2013 directive on attacks against information systems replaces a former legal instrument on cybercrime; the 2005 framework decision on attacks against information systems. This 2005 framework decision approximated the criminal law systems of the EU member states (by proposing definitions for illegal access to information systems, illegal system interference and illegal data interference) and enhanced cooperation between judicial authorities. With regard to jurisdiction, the text foresaw that each member state has jurisdiction for offences committed on its territory or by one of its nationals, but that whenever several states have jurisdiction over one single offence, they must cooperate to decide in which jurisdiction proceedings will be conducted. Member states

---

were required to exchange all information intended to enhance cooperation. Notably, national operational points of contact, available twenty-four hours a day and seven days a week, were to be appointed. Moreover, the 2005 framework decision established an obligation for states to prosecute in case it does not extradite its own nationals, an example of the earlier mentioned principle of *aut dedere aut judicare*.

The framework decision also listed the factors that should be taken into consideration in case one or more states have expressed a desire to prosecute:

> 'Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate cooperation between their judicial authorities and the coordination of their action. Sequential account may be taken of the following factors:

- the Member State shall be that in the territory of which the offences have been committed according to paragraph 1 (a) and paragraph 2,
- the Member State shall be that of which the perpetrator is a national,
- the Member State shall be that in which the perpetrator has been found.'

(Article 10(4) framework decision 2005 on attacks against information systems)

The recently adopted 2013 directive on the same subject matter has continued the approach to put forward rules of cooperation for a specific type of offense, rather than a general instrument. This approach might prove more fruitful than the earlier mentioned framework decision on jurisdictional conflicts, which covers a broad range of crimes, but does not put forward any binding rules. We will highlight the most important aspects of the document here, but it has to be kept in mind that its success in practice will have to be awaited, as the directive does not have to be implemented into national law until 4 September 2015.

---

23 Article 10(3) states that: 'A Member State which, under its law, does not as yet extradite or surrender its own nationals shall take the necessary measures to establish its jurisdiction over and to prosecute, where appropriate, the offences referred to in arts. 2, 3, 4 and 5, when committed by one of its nationals outside its territory.'

24 Directives have taken over the role of framework decisions in EU criminal law after the 2009 Lisbon Treaty.

25 The most important issue with this type of instrument has proven to be the sometimes rather 'liberal' implementation by states (i.e. the text of the instrument was not always strictly followed). A good example is the implementation of the European Arrest Warrant, see M. Fichera, The Implementation of the European Arrest Warrant in the European Union: Law, Policy and Practice (Intersentia, 2011).
The 2013 directive aims to amend and expand the provisions of the (previous) 2005 framework decision (in fact, it replaces the framework decision in its entirety). The amendments are substantial, as will be highlighted below, but also the nature of the new instrument offers advantages (a directive has direct effect whereas a framework decision does not).

If we turn to the substance of the directive Article 1 notes as to the general purpose of the instrument:

‘The directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities’ (emphasis added).

After defining the terminology, the directive requires states to criminalise the acts specified therein, as well as imposing a certain level of punishment. Interesting for our purposes here is Article 12 on jurisdiction:

1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:
   a. in whole or in part within their territory; or
   b. by one of their nationals, at least in cases where the act is an offence where it was committed.

2. When establishing jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction where:
   a. the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or
   b. the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State shall inform the Commission where it decides to establish jurisdiction over an offence referred to in Articles 3 to 8 committed outside its territory, including where:
   a. the offender has his or her habitual residence in its territory; or
   b. the offence is committed for the benefit of a legal person established in its territory.

(Article 12 directive on attacks against information systems)

The third paragraph of this provision obliges a state that decides to establish jurisdiction over an offence covered by the directive to inform the Commission (under the circumstances listed under a and b). The concept of enabling a third ‘neutral’ party to mediate between states in case of conflicting claims of jurisdiction is a potentially powerful mechanism. However, the directive does not go further than requiring states to ‘inform’ the Commission. If the Commission does not have any binding power (or binding guidelines to determine what state is best positioned for prosecution), all it can do it is make a recommendation.
Article 13 establishes a platform for the exchange of information in the form of a network of national contact points. Setting up a network of national contact points is a mechanism similar to Eurojust, which has been a great success as states have widely used the opportunity to strengthen cooperation by improving communication. Such a platform of informal cooperation has proven to have great potential. One of the questions it begs though is whether these particular crimes could not have been brought within the already existing platform of Eurojust. This would have possibly saved resources, as well as enabling states to make use of channels that have proven to be fully functional.

In addition to the issues on jurisdiction highlighted in this section, we will see a number of further issues related to jurisdiction below in section 12. In section 9 on the position of the individual, we will have a closer look at the concerns raised by legal instruments on cooperation, like the examples presented here, that pay little or no attention to the position of the defendant.

B. Mutual legal assistance and cooperation

5. European Convention on Mutual Assistance in Criminal Matters

In the next sections examples of mutual legal assistance (MLA) will be highlighted that could potentially contribute to the development of cooperation mechanisms between DPAs. Mutual legal assistance can present itself in many different forms but generally facilitates the gathering and exchange of information in an effort to support another state in the enforcement of criminal laws. Next to the many forms it can take, mutual legal assistance can take place at various levels, for example bilateral or multilateral treaties have been adopted, but agreements have also been adopted in the framework of international organisations.

Most important for our purposes here is the Council of Europe 1959 Convention on Mutual Assistance in Criminal Matters. The treaty was linked to the adoption of the previously mentioned Convention on Extradition, as

---

26 'For the purpose of exchanging information relating to the offences referred to in Articles 3 to 8, Member States shall ensure that they have an operational national point of contact and that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer,' Article 13 directive, supra note 20.

27 See section 10 below.

traditionally legal assistance and extradition were dealt with in the same instrument, but here was opted for two separate instruments. The reason for this was that it was expected that it would be easier for states to ratify this convention, rather than the treaty on extradition, which involves much more sensitive issues and may result in a possible loss of sovereignty.

Article 1 of the Convention does not limit its scope to a certain type of crime, therefore any crime can serve as the basis for a request for assistance. Contrary to the Convention on Extradition, which has a limited material scope. The purpose of such a broad scope was to also enable legal assistance for less serious crimes. The Convention defines this wide scope as:

‘The Contracting Parties undertake to afford each other, in accordance with the provisions of this Convention, the widest measure of mutual assistance in proceedings in respect of offences the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Party.’ (Article 1 Convention)

The Convention’s main aim is to establish a general obligation for its states parties to provide mutual assistance. The mutual assistance measures listed in the convention are therefore not exhaustive. Thus, a state cannot refuse assistance for the sole reason that the form of assistance requested is not listed in the instrument. The contracting states are obliged to provide ‘the widest measures of mutual assistance in proceedings’. This general obligation is subject to the exceptions of general principles of law, the grounds for refusal listed in the Convention and the limitations in the specific provisions on assistance. However, an obvious problem posed by a legal text without detailed provisions on the kind of collaborative acts that are required is how the assistance should be provided. In order to overcome such problems, the 1990 Schengen Convention and the 2000 EU Convention contain more detailed provisions on the kind of assistance that can be given (below).

Before discussing these developments, we will devote a paragraph to the general principles relevant to mutual legal assistance as they can be derived from the 1959 Convention. The principles in the 1959 Mutual Assistance Convention show similarities with those contained in the 1957 Extradition Convention, though in a weaker form. Generally speaking assistance is seen as less risky (i.e. no significant loss of sovereignty) compared to extradition and the requirements and principles tend to be more flexible. Like with extradition, these principles therefore are based on international law but are nowhere formulated in a binding form. They are derived from legal texts that states conclude. None of these texts are identical.
6. General Principles of Mutual Legal Assistance in Criminal Matters

Reciprocity

The principle of reciprocity underlies cooperation based on the Mutual Assistance Convention. It is generally accepted under international law that states cannot be forced to cooperate unilaterally. This implies that states only assist when the other state would do the same if a similar request was made to them (reciprocity). Being a signatory to the Convention does satisfy the requirement of reciprocity.

Nevertheless, reciprocity will have less of an effect in cases of mutual assistance than it has in extradition cases, especially considering the large variety of potential ‘assistance’ measures. An example: requests for investigating measures that the requested state would have never applied on its own accord, a strict application of reciprocity would in that case prevent assistance. However, the contracting parties have obliged themselves by signing the Convention to provide ‘the widest measures of mutual assistance in proceedings’.

As regards reservations (by making a prior statement) to the Convention, here also the principle of reciprocity applies (Article 23 (3)).

Double Criminality

Double criminality (the rule which prescribes that the offence for which assistance is sought is punishable in both requesting and requested states) is, as seen above, an absolute requirement in classical extradition law. The Mutual Assistance Convention does not explicitly require double criminality. So states can cooperate even when double criminality is lacking.

However, the Convention does allow for states to make a declaration stating that they require double criminality for the execution of (certain) forms of assistance. The option was included because in some states infringements of for example rights to property and privacy are to be applied strictly and only allowed in case of criminal conduct. Still, a certain degree of flexibility characterises the application of these traditional principles of international law, especially when compared with extradition. This is good news for data protection law, also in the EU. Many states with data protection laws have introduced data protection crimes, but the number of crimes introduced differs and the nature of these crimes is diverse.29 This state of affairs will not prevent these countries from providing each other mutual legal assistance once they decide to prosecute these crimes via the criminal way.

29 De Hert, supra note 2.
Speciality

The Mutual Assistance Convention does not contain an explicit provision on the rule of speciality; a common rule in extradition law prescribing that a person who is extradited is subject to prosecution only for those offences for which she or he was surrendered. However, some implicit reference to this rule can be found in for instance Article 12 of the convention:

‘A witness or expert, whatever his nationality, appearing on a summons before the judicial authorities of the requesting Party shall not be prosecuted or detained or subjected to any other restriction of his personal liberty in the territory of that Party in respect of acts or convictions anterior to his departure from the territory of the requested Party’.

Another example can be found in Article 6 (2) of the Convention, according to which: ‘Any property, as well as original records or documents, handed over in execution of letters rogatory shall be returned by the requesting Party to the requested Party as soon as possible unless the latter Party waives the return thereof’. The requested state is guaranteed that the documents will not be used for purposes other than those that served as the basis for the assistance. The principle is however not absolute, as the requested state can waive the return of the documents.

Grounds for Refusal

A similar flexibility applies to the grounds for refusal. Two groups of grounds for refusal can be found in the Mutual Assistance Convention, general grounds for refusal which apply to all forms of assistance, and the specific grounds which only apply to specific measures of assistance. A number of ‘traditional’ grounds for refusal, as contained in the Extradition Convention, do not apply to mutual assistance. The Mutual Assistance Convention does not allow for more traditional grounds for refusal such as the refusal to assist in cases concerning own nationals, and territorial limitations. However, reservations made by contracting states need to be considered as these can still introduce such grounds for refusal. In addition, Article 2 (b) of the Convention provides for a wide ground for refusal: ‘if the requested Party considers that execution of the request is likely to prejudice the sovereignty, security, ordre public or other essential interests of its country’. This general ground for refusal serves as a counterbalance to the wide obligations laid out by the Convention. Next to this general ground for refusal more specific grounds can be found in Articles 3–10 and 21–22. These grounds concern for example the so called ‘letters rogatory’ and the appearance of witnesses, experts and prosecuted persons. Regarding these grounds for refusal it can be noted that these are useful, or maybe more accurate; necessary. Political realities and differences between national legal
systems require such possibilities to refuse cooperation; when a nationally sensitive issue arises, a state can decide to halt cooperation. Recognition of such realities is important for cooperation between DPAs as well, as in this field similar political sensitivities and national interests are at play.

7. Using the criminal apparatus for cooperation in the field of administrative sanctions

The scope of the Mutual Legal Assistance Convention has been widened by the adoption of several protocols. In 1978 the 1st protocol was adopted,\textsuperscript{30} which limited refusal grounds for fiscal crimes and widened the scope of assistance measures regarding documents that can be requested based on the Convention. More interestingly for our purposes is the 2\textsuperscript{nd} protocol, which was adopted in 2001,\textsuperscript{31} and widens the scope of the Convention to also administrative sanctions.\textsuperscript{32} This has been an important move since administrative law frequently intervenes in criminal law, and the two fields have become intrinsically linked, making it in some cases even difficult to determine what actions belong to what field.\textsuperscript{33} Widening the scope in this manner was not a complete novelty (see next section), but it does allow for administrative cooperation to take place on the broad ‘Council of Europe’ level and even outside as the 2\textsuperscript{nd} protocol has already been ratified by more than 25 states, including Chile and Israel. This widening of the scope of the Mutual Legal Assistance Convention could be of special interest to data protection law, which is developing an administrative law approach, \textit{i.e.} administrative sanctions to data protection breaches. If this continues DPAs could where relevant make use of the framework of the Mutual Legal Assistance Convention, provided they are state parties to the convention and have ratified the 2\textsuperscript{nd} protocol.

The 2\textsuperscript{nd} Protocol furthermore expands the scope of the Convention to more ‘modern’ forms of cooperation such as video interrogation and joint investigative teams. This brings us to the next section, which is devoted to the trend (as observed \textit{above}), to a more detailed arrangement of assistance in this legal area.


\textsuperscript{31} Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, 8 November 2001, CETS No. 182.

\textsuperscript{32} See Article 1(3) ‘Mutual assistance may also be afforded in proceedings brought by the administrative authorities in respect of acts which are punishable under the national law of the requesting or the requested Party by virtue of being infringements of the rules of law, where the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters’.

8. More precise phrasing of powers in 1990 Schengen and 2000 EU Convention

The 1985 intergovernmental Schengen Agreement concerning the abolition of border checks was followed up with an 1990 implementing Convention.\(^{34}\) This convention was aimed at making mutual assistance between its contracting parties more flexible. Both extradition and mutual assistance are contained in the convention and serve as a complement to the already existing arrangements of the Mutual Assistance Convention by introducing a number of changes.

First, the implementing Convention extends mutual assistance to administrative sanctions,\(^{35}\) which was a revolutionary step for the time, as Protocol 2 to the Mutual Assistance Convention was not agreed upon until 2001. Article 49 furthermore applies to:

- b. in proceedings for claims for damages arising from wrongful prosecution or conviction;
- c. in clemency proceedings;
- d. in civil actions joined to criminal proceedings, as long as the criminal court has not yet taken a final decision in the criminal proceedings;
- e. in the service of judicial documents relating to the enforcement of a sentence or a preventive measure, the imposition of a fine or the payment of costs for proceedings;
- f. in respect of measures relating to the deferral of delivery or suspension of enforcement of a sentence or a preventive measure, to conditional release or to a stay or interruption of enforcement of a sentence or a preventive measure. (Article 49(b–f) Schengen)

Second, Article 50(1) enables mutual legal assistance ‘as regards infringements of their laws and regulations on excise duties, value added tax and customs duties.’ The principle of double criminality cannot be used to deny assistance based on this provision’s second paragraph. The abolition of double criminality extends the scope of the regime of Article 50, and in paragraph 3 the rule of specialty is clarified: ‘The requesting Contracting Party shall not forward or use information or evidence obtained from the requested Contracting Party for investigations, prosecutions or proceedings other than


\(^{35}\) See Article 49(a) of the Implementing Agreement: ‘Mutual assistance shall also be afforded: in proceedings brought by the administrative authorities in respect of acts which are punishable under the national law of one of the two Contracting Parties, or of both, by virtue of being infringements of the rules of law, and where the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters.’
those referred to in its request without the prior consent of the requested Contracting Party'. A breach of the principle of specialty would thus require the consent of the requested state.

Third, the Schengen convention eases the strict requirements of the 1957 Mutual Assistance Convention as regards letter rogatory:

‘The Contracting Parties may not make the admissibility of letters rogatory for search or seizure dependent on conditions other than the following:

a. the act giving rise to the letters rogatory is punishable under the law of both Contracting Parties by a penalty involving deprivation of liberty or a detention order of a maximum period of at least six months, or is punishable under the law of one of the two Contracting Parties by an equivalent penalty and under the law of the other Contracting Party by virtue of being an infringement of the rules of law which is being prosecuted by the administrative authorities, and where the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters;

b. execution of the letters rogatory is consistent with the law of the requested Contracting Party'. (Article 51 Schengen)

The requirement under (a) lowers the threshold of the 1957 Convention for letters rogatory, as a result these letters can be used for a broader range of offences within the Schengen countries.

Fourth, the 1990 Convention implementing Schengen allows in Article 52 to directly send procedural documents by mail to persons who are in the territory of another state. This provision is aimed at communication between authorities in one state with witnesses or experts in another state. Furthermore, it is required that the contracting parties send the executive committee a list of the documents which may be forwarded in this way.

Fifth and lastly, the implementing Convention eases relations between Schengen states in Article 53(1) as ‘Requests for assistance may be made directly between judicial authorities and returned via the same channels'. Requests, as well as decisions on these requests, can be handled directly between judicial authorities.

Ten years after the Schengen implementing Convention, a new boast to mutual legal assistance was given by the ambitious 2000 EU Convention on Mutual Assistance. The 2000 Convention is general in character and supplements and facilitates already existing instruments. A number of interesting


innovations were introduced by the convention and it especially aimed at clarifying and streamlining mutual legal assistance. These innovations were-driven by technological developments of the time. A good example: the Convention’s provisions on the interception of telecommunications (Articles 17 to 22), which set out in detail how such interceptions are to take place. No such provisions were to be found in any of the previous instruments, which the 2000 convention aims to supplement. Another innovation by the 2000 CONVENTION is that, even though limited, for the first time a mutual legal assistance instrument regulates the protection of personal data exchanged between states (Article 23). The Convention restricts the purposes for which personal data communicated or otherwise obtained under the provisions of the Convention may be used. Such data may be used only for the purposes of proceedings to which the Convention applies, other directly related proceedings, or ‘for preventing an immediate and serious threat to public security’. For all other purposes the consent of the subject or the consent of the communicating state must be secured. Where conditions have been imposed in the context of transfer of data, they will prevail over the provisions of Article 23.

C. Individual rights in inter-state criminal justice cooperation

9. The position of the individual in criminal justice cooperation

While cooperation instruments, both at the international and EU level, have undeniably improved efficient cooperation, they have often forgotten to address the position of the individual subjected to those measures (the suspect, defendant or convict). Individuals can find themselves investigated by and sent to foreign jurisdictions, of which they don’t speak the language, and often they will be detained awaiting trial, possibly for long periods of time. Moreover, positive conflicts of jurisdiction and the lack of a binding mechanism to solve these have also led to due process issues, particularly when no state takes responsibility over a cross-border investigation which leads to legal uncertainty for the individual.\(^38\) The cooperation measures adopted in the EU framework have been unbalanced and aimed at improving prosecutorial powers. A good example of extending prosecutorial power without due regard to individual rights is the sharing of evidence as a result of a transnational investigation.\(^39\) This raises issues as to what qualitative stand-

---


ards the gathering and admissibility of evidence should be held, as well as more general issues such as how investigative powers should be distributed among several jurisdictions and the related challenge of offering those affected by such measures a fair standard of justice. The coming into being of new modes of cooperation on a global scale has led to ‘an unprecedented mode of transnational collection of evidence by joint investigation teams’, and on the EU level

‘the improved MLA system has rapidly developed into the order model by means of the general enshrinement by EU legislation of the principle of mutual recognition as the cornerstone of almost the entire area of judicial cooperation, regardless of the very different nature of the judicial products concerned.’

This rapid growth in investigative measures has certainly improved the efficiency of international cooperation. But even though these can have far-reaching effects on individuals subjected to transnational investigations, no coherent international effort has been made to balance these effects by introducing procedural measures protecting the rights of the individual.

At the EU level this deficit has been recognized. After years of negotiation on a proposed measure that ultimately never saw the light of day, a series of procedural rights measures have recently been adopted under the roadmap on criminal procedural rights. However, whether these prove to be sufficient and create the balance that one would expect in a true area of justice remains to be awaited. When developing a new framework of cooperation, one would expect that in a rule of law the position of the individual and the safeguarding of fundamental rights would take a central role. This is a clear lesson that can be taken from the recent developments in EU criminal law cooperation and would have smoothened cooperation from the early beginnings, knowing that other states require at least an equal level of human rights protection.

---

40 Ibid., pp. 148–149.
41 See ibid., p. 151.
Double jeopardy (*ne bis in idem*)

Important to mention in the light of the above is the principle of *ne bis in idem*, also known as (the prohibition of) double jeopardy.\(^45\) This principle does not contain any rules on determining what jurisdiction is better placed to bring a case,\(^46\) but it works more as a limitation on criminal law enforcement, once a person has been (finally) judged for the same conduct in another jurisdiction, a second prosecution is barred.

Thus, the double jeopardy rule prohibits the prosecution of an individual for acts which have already been finally disposed.

The international variant of the principle is contained in various human rights treaties and is also contained in the EU Charter of Fundamental Rights. *Ne bis in idem* has been considered by the Court of Justice of the EU as a general principle of EU law,\(^47\) and regards dual prosecutions as obstacles to freedom of movement.\(^48\) The Court has given a broad interpretation to the meaning of ‘final disposal’.\(^49\)

For application between EU states the Article 54 Schengen Implementing Agreement is most important.\(^50\) Article 54 provides for an international rule of *ne bis in idem*, therefore when a case has been finally disposed, prosecution for the same offence is barred not only in the state where the judgment was handed down, but in all states parties to that treaty.\(^51\)

Thus, an EU-wide *ne bis in idem* rule limits double prosecution throughout the EU. In the international setting no such rule exists and its reach generally has only internal effects (within one jurisdiction),\(^52\) nevertheless, it is sometimes contained as a ground for refusal in extradition treaties.


\(^{48}\) Joined Cases C-187/01 and C-385/01 Gözütok and Brügge (2003), par. 38.

\(^{49}\) The Court has limited its reach though where a decision on the merits of the case has not been made, but prosecution has been abandoned to favour an ongoing prosecution in another member state, that decision does not bar the other prosecution, see e.g. C-469/03 Miraglia (2005), par. 35.

\(^{50}\) Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders.

\(^{51}\) Article 54: ‘A person whose trial has been finally disposed of in one Contracting Party may not be prosecuted in another Contracting Party for the same acts provided that, if a penalty has been imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing Contracting Party’.

\(^{52}\) For a discussion of the different application of *ne bis in idem* in intra- and inter-jurisdictional setting see D. Bernard, ‘*Ne bis in idem* – Protector of Defendants’ Rights or Jurisdictional Pointsman?’, 9 Journal of International Criminal Justice (2011), pp. 863–880.
D. EU mechanisms facilitating criminal justice cooperation

10. Eurojust

The EU has established various mechanisms and platforms to enhance the cooperation between criminal law enforcement authorities. 53 Two of these, Eurojust and European Judicial Network, will be highlighted here. 54 Eurojust is a prime example of a successful coordination mechanism between law enforcement authorities at EU level. Article 85 Treaty on the Functioning of the EU (TFEU) provides that Eurojust’s mission

‘shall be to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more states or requiring a prosecution on common bases, on the basis of operations conducted and information supplied by the states’ authorities and by Europol’. 55

Eurojust is an EU body with legal personality and seats in the Hague. 56 The primary aim of Eurojust is facilitating and stimulating cooperation between the ‘competent authorities’ of the 28 EU states. Eurojust was founded in February 2002 by a Council Decision with the overall purpose of strengthening the EU’s fight against serious crime. More specifically, the four main reasons for its founding are: (1) countering serious and organised crime within the EU; (2) increasing the level of safety and security for EU citizens; (3) stimulating judicial cooperation between EU states; (4) and the need for a body that could cooperate with the European Judicial Network (on which more below).

The legal framework of Eurojust was lastly amended in 2009, mainly to strengthen Eurojust, but also to accommodate any possible future expansion of Eurojust. 57

The members of Eurojust are criminal justice experts and represent their member state of origin at Eurojust. Each national member is seconded by the

---


member state in accordance with its legal system, who is a prosecutor, judge or police officer of equivalent competence. The duration of their function is for a maximum of four years (un-renewable). The statute of the national members (and their employees) is part of the national law of the member state. The national members of Eurojust together form the College, the organ responsible for the organisation and operation of Eurojust. The College can act collectively, but also through one or more national members. Every national member has one vote in the College.

The most important competence of Eurojust is to provide assistance to investigation into and prosecution of serious, organised and/or cross-border crime, and can do this either on its own initiative, or when requested by a member state. The primary aim of these competences is to stimulate, improve and coordinate cooperation between national authorities. Eurojust provides support to these authorities whenever needed in cases which concern two or more states. In case of an agreement with a third (non-EU) state, Eurojust can also provide assistance in cases between an EU member state and a third state. Even in case such an agreement does not exist, Eurojust can still assist in specific circumstances in which there is an urgent need to provide assistance. In addition, Eurojust can also assist investigations or prosecutions that concern only one member state and the EU when either the Commission or the state itself has requested for this assistance.

As said, Eurojust is competent to assist investigations into, and prosecution of serious, organised cross-border crime. Eurojust is thus only competent in case of serious crime, for which a certain threshold has to be met, examples are cybercrime, fraud, corruption, money laundering, environmental crimes and criminal organisations. In addition to the general competence of Eurojust, it also covers the types of crime and the offences in respect of which Europol is at all times competent to act as well as other offences committed together with the types of crime and the offences referred to here and all forms of crime when assistance is requested by one of the EU states. An exception is cooperation in cases concerning child protection. The EU has decided that Eurojust can assist in cases that have a relation to children, even when it does not concern organised crime. In October 2007 a contact point for child protection issues was established at Eurojust. The contact point ‘shall become a center of expertise in judicial cooperation in cases concerning children’, and shall be available to support and advise the National Members when dealing with cases involving children. Focusing on issues important to Eurojust, the contact point shall raise awareness on child protection-related matters, disseminate relevant information and advice on the possible actions to be taken.

58 See Article 4 ibid. for the minimum threshold.
The primary tasks of Eurojust include: requesting national authorities to start an investigation or prosecution; set up a joint investigation team (JIT); and/or provide all the information relevant for a JIT to fulfill its tasks. Furthermore, Eurojust can request national authorities to initiate certain investigative measures and other measures that are justified with the purpose of prosecution of criminal activities. These are the primary tasks of Eurojust.

It is important to note that none of the decisions of Eurojust are binding, Eurojust can only advice national authorities. Eurojust can also provide assistance of a more ‘logistic’ nature, such as for instance interpretation and translation. It is exactly the non-binding nature of Eurojust that has made it successful. Member states can benefit from the contacts and network provided by Eurojust to cooperate in criminal investigations, at the same time it does not fear to lose its sovereignty or competence over the matter.

11. European Judicial Network

The European Judicial Network (EJN) is the second example of a mechanism, or maybe better said forum, for cooperation between judicial authorities.59 The EJN was founded in 1998 by the Council as a forum for cooperation in the fight against serious crime and opts for a decentralised, flexible and horizontal approach. The EJN was the first structured operational platform for cooperation in cross-border crime within the EU and functions as a horizontal network.

The EJN exists of a network of judicial contact points; either members of the prosecutorial service and/or representatives of the ministry of justice, who are available, from their own member state, to provide information on their own national criminal systems and the national judicial authorities. The contact points are not transferred to a common organ, like at Eurojust.In 2008, ten years after EJN was founded, a new Council Decision providing the legal framework for EJN entered into force.60 The general ‘spirit’ of the EJN was kept; it was only the legal position of EJN that was strengthened. Previously EJN was established by a soft law instrument (a common position), now it has a strong legal foundation, namely a Council Decision.

The three primary tasks of the EJN are: (1) enhancing networking between various contact points; (2) organising meetings of national representatives; (3) and a continuous provision of up-to-date legal and practical data/information, through an adequate network of telecommunication. EJN also provides a platform for direct communication in order to enhance interstate cooperation.

Next to providing this ‘network’, EJN contact points have individual tasks and responsibilities, they have to: (1) actively mediate between states to

---

59 For more on the EJN see, in Dutch, P. De Hert, et. al, supra note 1, pp. 60–62.
enhance cooperation, with the main purpose of preventing serious crime; (2) provide legal and practical data/information to foreign judicial authorities to enhance judicial cooperation in a specific case, or to improve cooperation more general; (3) and to improve the organisation of education about judicial cooperation in criminal matters by the national authorities.

Another instrument which has proven very useful in practice is the website of the EJN, which provides for various tools to improve cooperation among states. It for instance contains general information about how legal assistance is executed in the various states, a contact book with all information about contact points and a handbook with the various mutual recognition instruments.61

As can be noted from these short overviews of Eurojust and EJN, many parallels can be drawn between both bodies. They both consist of judicial contact points, and the secretariat of EJN is based within the premises of Eurojust. Most importantly they both are concerned with the enhancement of judicial cooperation in criminal matters between EU states.

The EJN Council Decision explicitly mentions the important relationship between the two bodies, and notes that its relationship is based on dialogue and complementarity. The information centralised by the efforts of EJN will be made available also to Eurojust, and when the EJN contact points believe that Eurojust is better positioned to deal with a case the national member of Eurojust will be informed. The national members of Eurojust can participate in EJN meetings, when invited by the EJN. The national terrorism correspondents at Eurojust can also use the secured telecommunication network of EJN.

12. The European Public Prosecutor’s Office

Next to extending Eurojust’s powers, as already stipulated above (Article 85 TFEU), the TFEU also lays out a legal basis for the creation of a European Public Prosecutor’s Office (EPPO) in Article 86.62 In short, the main role of the EPPO would be to investigate and prosecute crimes committed against the EU budget (such as EU-fraud, corruption, embezzlement and money laundering). In July 2013 the European Commission launched its legislative proposal to create an EPPO.63 The proposal has been heavily debated and even though it remains unsure what form (and with the support of which

---

member states) an eventual EPPO might take, it shows the spirit and intentions of the EU to move ahead with its plan for an enhanced form of EU criminal justice cooperation. A possible EPPO will pose a new set of challenges by setting up a prosecutor at the European level with the power to take almost any intrusive measure that a national prosecutor can, and its territorial jurisdiction will cover the combined territory of the states joining the initiative. A look at the recent proposal for an EPPO shows that fundamental rights protection is not among the core priorities. A conclusion shared by the Meijers Committee, which aptly notes:

‘Further interferences with national criminal procedure than now on the table are often considered to be disproportionate. To better embed legal protection, three aspects should be considered more closely by the co-legislators. First, the EPPO should contain clearer rules on the determination of the applicable law. Second, procedural guarantees should be updated to function effectively in transnational criminal cases. Third, rules on the gathering and admissibility of evidence should be developed further.’

Learning from past mistakes, it would seem wise to start an important new initiative like the EPPO with taking account of individual rights. Not only from a pragmatic viewpoint, i.e. to make cooperation effective in practice, but more importantly; respect for fundamental rights is one of the core pillars on which the EU rests. Recent history has shown that when the position of the individual is not given sufficient attention from the start, the fallout will be significant and it will take years and difficult political negotiations to even begin to overcome such deficiencies.

Overall, what can be taken from the EU experience of establishing agencies and platforms to facilitate cooperation is that next to legal instruments regulating cooperation between states, mechanism that in a sense are supranational are needed to guide states in their interaction. This guidance or coordination can be of a non-binding nature (such as Eurojust), but also of a binding nature (like the proposal for an EPPO). In practice a combination of the two might be most effective, binding where possible, but where the protection of national interests prevents states from entering into a binding mechanism (and this will in practice be in most areas, certainly in the early stages of protection between DPAs) a non-binding platform can prove valuable.


E. Discussion

13. What lessons can data protection draw from cooperation in criminal justice matters?

The political lesson

In this chapter we saw that international public law does not provide for any binding rules in the field of criminal justice cooperation, or at least not to the extent that states are bound without prior consent, firstly in the field of jurisdiction (part A), and secondly regarding mutual legal assistance (part B). In response to the jurisdictional issues, states have extended the reach of their national law by applying jurisdiction in a broad (extraterritorial) sense. As a result states are ‘independent’ (to an extent) in enforcing national criminal law, in some cases even when crimes have been committed partly or completely outside of a state’s territory. In cases in which national law is not sufficient, states engage in cooperation in the form of treaties, either bilateral or multilateral. Criminal justice cooperation mostly takes place within a pre-existing legal framework, ad hoc cooperation is rare. The legal framework regulating criminal justice cooperation is often an expression of differences between national legal systems and cultures. These differences take shape in the form of exceptions (or grounds for refusal) written into cooperation agreements (mostly in the form of treaties). These exceptions allow states to retain control over certain aspects that are regarded as fundamental, while it promotes cooperation where none of the exceptions apply. This might at first seem like limiting the reach of cooperation, but it is not. Especially in a field as sensitive as criminal law, but in cooperation more general, national differences have to be acknowledged. Without such recognition, cooperation would be very unlikely, as states often simply cannot do away with fundamental (constitutional) principles. Cooperation instruments (including grounds for refusal) in criminal law have resulted in an increase in efficiency and have enabled cooperation. In developing cooperation mechanisms between DPAs it would be extremely useful to think about principles and rules, as these help provide a realistic path towards fruitful cooperation.

The example of the EU is extremely important for our purposes here. The EU has aimed to enhance cooperation, with the ultimate purpose of automatic recognition of foreign judicial decision with abolished or minimised grounds for refusal. When there is a closer tie between certain states (like in the EU), it is easier to negotiate cooperation agreements than in a global setting. The same is true for cooperation between DPAs; cooperation within Europe will take shape along different lines than international cooperation. At the same time, even though EU states are part of the same ‘political family’, the differences between national legal systems and cultures are fundamental
and this has put a break on smooth cooperation. This shows that states cannot be ‘naïve’ in putting forward rules for cooperation, but even in the relatively integrated European Union it is important to keep in mind national differences. Because EU criminal law itself is in development and is still a relatively new form of integration no hard lessons can be drawn, but the experience with the EAW has shown that the initial approach of automatic cooperation was not feasible, subsequent cooperation measures (for example the European Investigation Order on the gathering and exchange of evidence) have therefore reintroduced certain grounds for refusal, acknowledging differences between national systems.

Taking the international and the European examples together, it seems that for a field of cooperation that still has to take shape (the case of DPAs), it would be wise to retain a ‘political element’ in cooperation measures. Allowing states to pull the emergency break when fundamental national rules and principles are threatened can prove a first step toward a workable cooperation framework.

**Legal lessons**

The downside of effective cooperation in criminal law has been the position of the individual, as briefly shown in part C. The increase in efficiency has often come at the expense of the suspect who sees his or her rights eroded by becoming a ‘subject’ of international cooperation. And even though within the EU measures have been adopted to improve defence rights and an EU-wide *ne bis in idem* rule prevents suspects from being prosecuted multiple times for the same conduct, this has not yet proven sufficient to balance the prosecutorial bias in cooperation measures. An area of justice cooperation cannot be viewed only from the interest of states (in the case of criminal law prosecution), the position of the individual has to be given the consideration it deserves right from the start.

Moreover, our contribution has highlighted a slow development towards precision in the legal texts on mutual cooperation. Detailed description of forms of cooperation where absent in the 1959 Convention on Mutual Assistance. Only towards the turn of the century, in particular with the 2000 EU Convention on Mutual Legal Assistance, care was taken to spell out the most important forms of cooperation that could be asked for between states, including the necessary legal guarantees for far going request such as carrying out telephone taps. The same 2000 Convention was also the first to pay attention to the need for data protection between cooperating authorities and

---

restricts the purposes for which personal data communicated may be used. Such data may be used only for the purposes of proceedings to which the Convention applies, other directly related proceedings, or ‘for preventing an immediate and serious threat to public security’. For all other purposes the consent of the subject or the consent of the communicating state must be secured. This was a significant improvement and shows that the framework’s modernisation does not only lead to benefits for prosecutors, but also for individual rights.

Another interesting lesson from the EU example, as demonstrated in part D, is that more informal (without binding powers) platforms of cooperation (like Eurojust) can prove extremely useful, and might provide a first step towards further integration (the development from Eurojust to the EPPO is this ‘further step’). In providing channels for cooperation and communication, Eurojust has proven to be well-functioning and strongly embedded in the EU legal culture. A mixed-model with on the one hand non-binding cooperation mechanisms, to enhance cooperation by way of central coordination, and on the other binding legal rules (for example the EAW), might be the way forward and presents an example of a valuable and workable system for cooperation between DPAs.
Towards efficient cooperation between supervisory authorities in the area of data privacy law

Dariusz Kloza, Antonella Galetta


1. Introduction

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

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

The need for improving cooperation to achieve efficiency is not disputed and debates about how to shape efficient cooperation have not come to a conclusion. This chapter aims to bring its own modest conclusion to the table. It builds on a previous contribution of similar nature, namely (Kloza and Mościbroda 2014), in which lessons for the enforcement cooperation of supervisory authorities in the area of data privacy law were drawn from analogous cooperation in the field of European competition law. Going beyond mere enforcement cooperation, we will propose 23 legal and practical recommendations that might help overcome contemporary inefficiencies. They are addressed, respectively, to policy-makers, i.e. regulators developing framework(s) and arrangement(s) for cooperation, and to supervisory authorities themselves, suggesting actions they could undertake; although this distinction is not often clear-cut. Having provided an overview of the state of the art of cooperation in data privacy law (Section 2), we will briefly

---


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

introduce the core elements that make the functioning of enforcement cooperation in competition law efficient (Section 3). Based on these findings, our main recommendations will be elaborated in Section 4, which also suggests an action plan concerning the development of efficient cooperation in data privacy law (Section 4.3). Our analysis aims to fuel discussion and, in particular, to inform the on-going reforms of European data protection frameworks. These recommendations are not exhaustive in nature and – as the PHAEDRA project continues till January 2017 – remain open for further discussion.

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

Some preliminary clarifications, however, are needed before digging into the topic of this chapter. First, our analysis is targeted towards an efficient cooperation amongst supervisory authorities, instead of an effective one. The expression “effective cooperation” is recurrent in data privacy law, effectiveness being the possibility or capability of producing a result. We rather argue for such cooperation to be efficient, efficiency being the possibility or capability of “functioning or producing effectively and with the least waste of effort.” Thus, we claim that cooperation initiatives should reach certain objectives but with the smallest possible waste of financial, human and technical resources, which are critical to supervisory authorities (European Union Agency for Fundamental Rights 2010). In so doing, we aim to strive for the highest possible cooperation standard in data privacy law. Second, following Kuner et al., we have consciously selected the the term “data privacy” – embracing in particular the European understanding of “personal data protection” and the Anglo-Saxon one of “informational privacy” – in order to “avoid terminology that might seem focused too much on a particular legal system” (Kuner et al. 2014). Third, for similar reasons, we have selected

8 Supra note 4.
9 Cf. e.g. Recital 11 as well as Articles 45–46, 55 and 66(1)(e) GDPR.
11 Ibid.
the term “supervisory authority”\textsuperscript{12} to indicate relevant public bodies tasked with the governance of data privacy in a given jurisdiction. The term we use here comprises data protection authorities (DPAs), privacy commissioners (PC), privacy enforcing authorities (PEAs) (Stewart 2013) and – a novelty in our “dictionary” – privacy enforcing agencies (Bygrave 2014).\textsuperscript{13} Only some of these bodies are independent regulatory authorities, while others may be public bodies tasked \textit{prima facie} with other issues, but dealing with data privacy too. We opt for this all-encompassing approach as independence is not always a requirement for cooperation in data privacy law and such cooperation may involve authorities at various levels. Still, we are aware that supervisory authorities are not endowed with the same functions and powers (Bennett and Raab 2006) as well as resources, which is often reflected in their willingness and ability to cooperate as well as in the scope thereof. (We are also aware that not only public bodies might be involved in the protection of data privacy, e.g. NGOs, but these do not focus on enforcement and thus fall outside the term “supervisory authorities”.) Fourth, by a “cross-jurisdictional data privacy violation” we refer to a breach of data privacy laws producing effects or implications in more than one jurisdiction. Finally, by “cooperation” we mean a spectrum of activities undertaken together by supervisory authorities in fulfilling their functions and duties. This cooperation is not of a uniform nature and can range from “soft” forms, such as policy shaping, exchange of good practice, training, study visits, research or education, to “hard” ones, like enforcement of data privacy laws in cross-jurisdictional cases. For (Baggaley 2014), these latter forms of cooperation can vary from: (1) sharing of non-confidential information, to (2) coordinated compliance activities, to (3) sharing confidential information, and to (4) formal enforcement cooperation (Fig. 1).

\begin{center}
\begin{tabular}{llll}
Sharing Non-Confidential Information & Coordinated Compliance Activities & Sharing Confidential Information & Formal Enforcement Cooperation \\
GPEN & GPEN Sweep Insecam Letter\textsuperscript{14} & Assisting with Unilateral Investigations & Joint/Coordinated Investigations \\
\end{tabular}
\end{center}

\textbf{Figure 1. The enforcement cooperation spectrum}


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

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

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

From the formal point of view, within the scope of data privacy laws, cooperation does often represent the sole means to effectively remedy data privacy violations. (Otherwise individuals would need to use other mechanisms, such as consumer law.) Speaking even more practically, a lack thereof usually entails a duplication of efforts in investigating and/or sanctioning violations, ultimately leading towards inconsistent enforcement. It follows that some of the duties performed by supervisory authorities – “by reason of the scale or effects” – might be better and more efficiently undertaken jointly with their counterparts.15

However, data privacy law is very much built upon the interplay among data subjects, data controllers or processors and supervisory authorities.

---

15 Here we have been obviously inspired by the contents of the principle of subsidiarity spelled out in Article 5 TEU: “Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.”
If follows that cooperation among supervisory authorities should not only be aimed at easing tasks and smoothing procedures, but also at strengthening data subject’s rights and benefit – or at least not damage – data controllers and processors.

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

1. Global Privacy Enhancement Network (GPEN),
2. European Conference of Data Protection Authorities (ECDPA; “Spring Conference”),
3. Article 29 Working Party,
4. Asia-Pacific Privacy Authorities (APPA),
5. Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement (APEC CPEA),
6. APEC Cross-Border Privacy Rules (APEC CBPR),
7. Association francophone des autorités de protection des données personnelles (AFAPDP),

24 Rather informal.
Still, the diagram illustrated at Fig. 2 is obviously not exhaustive. In fact, there are at least four additional cooperation frameworks that should be added, namely: (1) the framework created by the Council of Europe's Convention 108,\(^{25}\) (2) the International Conference of Data Protection and Privacy Commissioners (ICDPPC),\(^{26}\) (3) the International Working Group on Data Protection in Telecommunications (IWGDPT; ‘the Berlin Group’),\(^{27}\) (4) the Red Iberoamericana de Protección de datos (RIPD)\(^{28}\) and Central and Eastern Europe Data Protection Authorities (CEEDPA).\(^{29}\) Furthermore, one must complete this picture by adding numerous bilateral arrangements between various supervisory authorities and/or their networks.

---

3. Lessons from enforcement cooperation in European competition law

The analysis thus far leads us to the conclusion that cooperation among supervisory authorities in the area of data privacy law is still in its infancy and there is significant room for improvement. Hence, how would it be possible to make such cooperation more efficient? Our starting point would be to recall a few lessons learnt from enforcement cooperation in European competition law that would subsequently constitute a basis for a broader set of legal and practical recommendations.30

Enforcement cooperation in competition law31 shares a lot of similarities with its counterpart in data privacy law. First and foremost, globalization and developments in information and communications technologies (ICT) result in an increasing number of multi-jurisdictional cases and thus call for cooperation between relevant authorities. When it comes to cross-jurisdictional cases, both supervisory authorities in data privacy law and competition authorities have comparable needs: in both situations, in order to ensure efficiency and consistency, enforcement requires closer cooperation between competent authorities, e.g. assistance in evidence gathering and exchange of case-related information, including confidential or otherwise protected information. It is also likely that these two areas would face similar obstacles. Next, in both fields, certain basics for cooperation have been already developed: various formal and informal arrangements, of varying geographical reach, coexist (i.e. international, regional, and bilateral). In both fields, the convergence of legal frameworks facilitates cooperation, and vice versa (Kloza and Mościbroda 2014, 135). What differs these two is that enforcement cooperation in competition law has already achieved a relatively high level of efficiency while its counterpart in data privacy law still only aspires thereto.

Finally, it is European competition law that offers perhaps the most advanced, sophisticated and – what is sought in the data privacy area – efficient arrangement for enforcing its substantive provisions, which has

---

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

31 By “European” competition law, we actually mean the one of the European Union. Enforcement cooperation therein is based on Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 04.01.2003, pp. 1–25. Its entry into force substantially modernized the enforcement of European competition law, marking a transition to a more decentralized one; therefore means of cooperation between the European Commission (Directorate-General for Competition) and national competition authorities (NCAs) needed to be established.
proven useful over the past decade.\textsuperscript{32} It is the European Competition Network (ECN) – established and governed by a directly binding regulation – that enforces substantive European competition law. The ECN is an example of cooperation between relevant authorities based on a clear legal basis, setting forth clear procedures, including those for an exchange of confidential information, and thus allowing closer cooperation. For that reason, it became a worldwide reference point for cooperation in competition and antitrust enforcement (Kloza and Mościbroda 2014, 132).

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

A few of these criteria require some further explanation. It should be noted that a “firm legal basis” means that a legal instrument must be in place at national level and must satisfy certain criteria of both contents of the law and quality of law-making. From a broader perspective, this requirement can be translated into the principle of legality, which is rooted in Western liberal democracies. Among other international and European treaties, the principle of legality stems e.g. from the second paragraphs of Articles 8–11 of the Eu-


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

\textsuperscript{34} Emphasis ours.
European Convention on Human Rights (ECHR) and is recurrent in the case law of the European Court of Human Rights (ECtHR; Strasbourg Court). In particular, this case law refers to the interpretation of the expressions “in accordance with law” or “prescribed by law”, occurring in Articles 8–11 ECHR (Galetta and De Hert 2014). Although these deliberations are primarily applicable in cases of interference with a fundamental right, the conditions for the quality of law-making are equally applicable here. According to the established jurisprudence of the ECtHR, the phrase “in accordance with the law” [Article 8(2) ECHR] includes the following:

a. A norm cannot be regarded as a “law” unless it is formulated with sufficient precision to enable the citizen – if need be, with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail; however, experience shows that absolute precision is unattainable and the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague […].

b. The phrase “in accordance with the law” does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law; it thus implies that there must be a measure of protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by, inter alia, paragraph 1 of Article 8 […].

c. A law which confers a discretion is not in itself inconsistent with the requirement of foreseeability, provided that the scope of the discretion and the manner of its exercise are indicated with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference […].

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

---

35 ECtHR, Olsson v Sweden (No. 1), application No. 10465/83, judgment of 24 May 1988, § 61. The Court reached those findings in its previous cases Sunday Times v the United Kingdom, application No. 6538/74, judgment of 26 April 1979, § 47; Silver and Others v the United Kingdom, application No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, judgment of 25 March 1983, § 86; and Malone v the United Kingdom, application No. 8691/79, judgment of 2 August 1984, §§ 66–67.
of enforcement cooperation initiatives in data privacy law does not result in much concrete commitment and thus renders it inefficient.

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

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

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

4.1 Legal recommendations to the attention of policy-makers

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

The current legal framework on the basis of which supervisory authorities cooperate is a complex one. It required a large amount of research to identify the existing networks and to understand them and how they work. Our common sense suggests that if we spent quite some time to get to the bottom of this system, a lay citizen may hardly do so and will certainly encounter as many difficulties as we did. These difficulties become more concrete and tangible in case a lay citizen needs to contact one of those

---

^36^ Ironic.
supervisory authorities as data subject to exercise one of her rights and/or to remedy a data privacy violation. Such situation gets even more complicated if such a violation is of a cross-border nature. Yet, the complexity of the existing cooperation arrangements and frameworks has a negative impact not only on data subjects but also on the other actors involved in this “business” namely data controllers or processors and supervisory authorities. Supervisory authorities, often supported by in-house legal experts, would probably somehow figure out how the system works. So will big businesses and organisations, but small or medium enterprises (SMEs) might need to resolve to legal help.

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

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

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

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

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

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

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

---


38 “Conflict of laws” in the Anglo-Saxon terminology.


for supervisory authorities in data privacy law (however, we acknowledge this will require further analysis) or might inform the development of cooperation arrangements and frameworks.

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

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

These two core conditions are applicable to the whole “universe” of the protection of fundamental rights, including data privacy, and thus apply equally to the legal framework for the cooperation of supervisory authorities in the area of data privacy law. Moreover, Art 13 ECHR, ensuring the right to effective remedy, further safeguards such effectiveness. It stems from the Strasbourg Court case law that (Council of Europe 2013):

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

---

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

45 References to particular cases omitted. Cf. further: ECHR, *Silver and Others v the United Kingdom*, application No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, judgment of 25 March 1983, § 113. ECHR, *Leander v Sweden*, application No. 9248/81, judgment of 26 March 1987, § 77; (European Union Agency for Fundamental Rights 2014, 15–17).
4. “The user is always right” (popular adage). The closer to the individual the case is solved, the better. The arrangement(s) and/or framework(s) should be user-friendly.

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

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

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

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

Data privacy is a cross-cutting subject and data subject’s rights may deserve protection under different bodies of law such as consumer protection law, competition law, equality law, criminal law, etc. This reflects the need to establish and develop forms of cooperation among different actors in these fields, also beyond borders of a single jurisdiction. These actors

47 Supra note 35.
would include relevant supervisory authorities, judicial authorities and administrative bodies as well as non-state actors, such as NGOs. Various networks and associations of these actors should be invited to cooperate as well.

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

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

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

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

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

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

49 In classical terms, having extraterritorial jurisdiction means to be able to “exercise […] jurisdiction […] over activities occurring outside […] borders” (Senz and Charlesworth 2001), but – in the digital era – it shall rather refer to “the exercise of jurisdiction (that may well, but need not, be extraterritorial) [that] has any extraterritorial effect or implications” (Svantesson 2013).
These authorities should have both subject-matter jurisdiction (i.e. the one over the type of a dispute concerned; *ratione materiae*) and personal jurisdiction (i.e. the one over the parties involved; *ratione personae*), but this ability cannot be unlimited. Svantesson argues that “extraterritorial jurisdictional claims are reasonable because if states do not extend their data protection to the conduct of foreign parties, they are not providing effective protection for their citizens” (2013).

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

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

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

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

Data controllers and processors, especially in the private sector, might wish to escape the possibility of being held liable for cross-jurisdictional data privacy violations by choosing the place of establishment in a jurisdiction where a supervisory authority does not cooperate with its foreign counterparts or where the level of data privacy protection is simply lower.
They often view this scenario as an invitation to “shop” for a more favourable forum. Such a situation is often detrimental for the data subject. We see two problems here. First, if enforcement cooperation remains voluntary, some authorities might not wish to engage. In this situation, it is very likely that the enforcement of data privacy law would be stricter in those jurisdictions in which cooperation initiatives are in place and looser in those in which no such framework is in place.

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

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

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

While the need for sharing information in enforcement cooperation in cross-border cases is hardly contestable, the problem of relevance of information might occur. In our view, it is not that all information related in one way or another to a case being dealt with would need to be exchanged among the authorities concerned. Rather, supervisory authorities should be able to determine themselves, on a case by basis, what constitutes relevant information before sharing them with their counterparts and provide justification therefor. If supervisory authorities have divergent opinions about relevance of information, they should be able to negotiate about that, to the extent permitted by law. (E.g. perhaps under no condition

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

The problem here is not about data privacy laws as such, which are usually silent about any type of confidential or otherwise protected information (short of personal data themselves), but rather about national administrative laws, both substantive and procedural, that preclude sharing information in given situations.
authorities would share state secrets, but some other types of information, e.g. trade secrets, might be exchanged if higher safeguards are ensured. The latter might include for instance retention periods, limitations on use and further disclosure, and an obligation to ensure security and confidentiality. 

9. “The piano keys are black and white, but they sound like a million colours in your mind” (Katie Melua). Cooperation among supervisory authorities should rely on comprehensive and harmonised legal “tools” and procedures to be used in cross-border cases. Extra-legal tools should supplement legal ones. To that end, some minimal “table of contents” for any arrangement(s) and/or framework(s) should be agreed in a first place.

As of now, supervisory authorities have at their disposal a wide range of legal “tools” to be used in cross-border cases. A quick survey of these tools reveals, among others, joint investigations, sharing evidence, audits, class action litigation, privacy certification and seals. Yet, these tools are far from being harmonised, i.e. they might be at disposal of one of the authorities cooperating, but not of the other. Furthermore, one authority might not be able to accept some requests from its counterpart.

The harmonisation of these tools, supplemented by the approximation of relevant procedural norms, would strengthen enforcement in data privacy law. The biggest problem is to make a list of “items” this harmonisation should concern. We have found the 2010 APPA Cross-border Privacy Enforcement Arrangement (CPEA) to be one of the first instruments containing one of the most comprehensive suggestions, i.e. procedures for cross-border cooperation (§9), respecting and safeguarding confidentiality (§10), information sharing, including contact point designation and sharing experience (§11), and miscellaneous matters such as staff exchanges, costs, and disputes (§§12–15). The non-binding Global Cross Border Enforcement Cooperation Arrangement, adopted at 36th ICDPPC at Mauritius, can serve here as another example. It deals with issues ranging from reciprocity, confidentiality and respecting privacy and data protection principles, to coordination principles, resolving problems and allocation of costs, to the return of evidence and eligibility.

Similarly, the harmonisation of tools prima facie not concerned with enforcement can be of some use too, such as cross-border data breach notifi-
cation, privacy and data protection impact assessments (PIA, DPIA), privacy enhancing technologies (PETs) and binding corporate rules (BCR). The same is true for “soft” measures, such as “naming and shaming” and guidance.

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

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

Although supervisory authorities already rather know each other – at the end of the day, the worldwide data privacy community is rather small – they should know more about themselves. Yet, as a prerequisite, they should not discriminate their counterparts and genuinely treat them as peers, i.e. there is no more “important” or “influential” authority in the community.54 To that end, first, they should know more about the enabling laws of their counterparts. This should include also soft law instruments (e.g. best practice) and those originating from international bodies, both formal and informal, e.g. ICDPPC, as well as practical documents (e.g. templates). We acknowledge the existence and benefits of several databases fed with such information (e.g. the International Privacy Law Library run by the World Legal Information Institute).55 However, some of these databases are selective, not easily accessible or accurate or simply they are not yet widely known nor used. The key here is comprehensiveness: such a database should cover as many jurisdictions as possible, should be regularly updated and widely referred to. In addition, a manual or guidelines could append such a database, in particular summarising key knowledge about each supervisory authority. This will allow supervisory authorities to determine, in a first place, if they can engage in cooperation and in what type thereof, and, subsequently, roles, competences, powers, responsibilities and procedures used by their counterparts.

Second, although we assume all supervisory authorities have already exchanged their contact details (e.g. within WP29, CoE or GPEN), they

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

should make sure they have designed contact points for each of the purposes of cooperation, e.g. for handling cases (enforcement), for public education and/or for mutual training. Such a contact list should not only include the top officials, but also key staff, especially those in charge of international relations and enforcement. It should be kept up-to-date.

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

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

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

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

12. “An ounce of prevention is worth a pound of cure” (Benjamin Franklin). Supervisory authorities should take the lead in preventing data privacy violations from occurring, including cross-border ones, rather than
focusing solely on *ex post* investigation and prosecution. Therefore, cooperation should be extended to all of their powers and duties, and should not regard only enforcement. This recommendation is meant for policy-makers and supervisory authorities to pay equal attention to the forms of cooperation other than enforcement, such as public education and internal trainings as well as contribution to policy-making and standard setting, with a view to more efficiently protect data privacy. Initiatives such as the European Data Protection Day,\textsuperscript{56} the Privacy Awareness Week\textsuperscript{57} or the ARCADES project\textsuperscript{58} have proven useful. Likewise, the strengthening of preventative tools such as privacy and data protection impact assessments may help reach this purpose (cf. Recommendation 9).

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

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

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

Although this provision should be welcomed, it is unclear how EU Member States would be able to ensure “adequate” resource endowments. Simi-


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

larly, it is not yet clear which criterion will be used by Member States to fix that target.

14. “A man with a conviction is a hard man to change” (Leon Festinger). Supervisory authorities must be genuinely convinced that engaging in cross-border cooperation is beneficial for the mission they realize. Motivation is key in any cooperation initiative and represents its baseline. Supervisory authorities do not usually engage themselves in cooperation unless they share common interests and concerns (Barnard-Wills and Wright 2014). Although this is more than reasonable, we find that cooperation is needed in cross-border cases, regardless of whether or not a supervisory authority expressed prior interest in a certain issue or topic. Moreover, if supervisory authorities cooperate efficiently and effectively, there is no better result or outcome each of them would have reached alone. Yet, it has to be recognised that cooperation requires some prerequisites such as trust among peers, commitment, communication, regularity of interaction and inclusiveness, which cooperation itself cannot guarantee.

15. “Deine Zauber binden wieder” (Friedrich Schiller). The worldwide cooperation of supervisory authorities in the area of data privacy needs encouragement from the authorities themselves as well as from policymakers, in particular from international and supranational ones, such as the OECD, APPA, Council of Europe or the European Union. These bodies should set (a) standard(s) for efficient cooperation, perhaps one(s) to be formalized.

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

16. “Training is everything. The peach was once a bitter almond; cauliflower is nothing but cabbage with a college education” (Mark Twain). Supervisory authorities should continue to enhance their efforts in mutual exchange of know-how by means of study visits, seminars and/or staff exchange. Any effort to exchange know-how among supervisory authorities should be welcomed and should be encouraged as means towards the efficiency of cooperation. The mutual exchange of expertise and competences should be promoted at all levels and be targeted to any person working within supervisory authorities, from senior managers to secretaries. Fellowship programmes, for instance, are fit for this purpose. For example, the FTC has established the International Fellows Program, which – since 2007 – has hosted 52 staff members from sister agencies around the world.\(^6\) However, it should be recognised that not all supervisory authorities have enough resources to finance these programs and/or are lucky enough to have access to them. In this latter case we find that seconded national experts programs, which are quite common in the public sector, represent the most appropriate solution. These programs would allow for the mutual exchange of expertise, but without too much burden for the supervisory authority hosting the “external” expert.

17. “Et je voudrais pouvoir un jour enfin te le dire, te l’écrire, dans la langue de Shakespeare. (...) Je ferais mieux d’aller choisir mon vocabulaire pour te plaire dans la langue de Molière” (Charles Aznavour). Supervisory authorities need to clearly understand themselves, their work and their “clients”, i.e. data subjects and data controllers or processors. Despite English being almost the lingua franca, they need to establish procedures for interpretation and translation of meetings and information shared. Cross-border cooperation of any type will engage supervisory authorities using different languages. In order to ensure effective and smooth communication, procedures for translation and interpretation must be established. A few possible scenarios:

1. in their communication, authorities might select a single language or choose “bridging” languages, a solution somehow known from patent law, in which the core of a patent document (i.e. patent claims) should be published in English, French and German;\(^6\)


\(^{61}\) “The official languages of the European Patent Office shall be English, French and German. [...] A European patent application shall be filed in one of the official languages or, if filed in any other language, translated into one of the official languages in accordance with the Implementing Regulations”; Article 14(1)-(2) of the Convention on the Grant of European Patents (Munich, 5 October 1973), http://www.epo.org/law-practice/legal-texts/epc.html.
2. supervisory authorities, for the purposes of sharing information, while
determining its relevance, might translate it to the recipient’s language;
3. a data subject might be offered to address her complaint concerning
a cross-border violation in her own language or in English (or any other
“bridging” language). The advantage for the data subject to opt for English
is that most probably in this latter scenario her case will be dealt faster. Yet,
supervisory authorities themselves have to make sure that the right to an
effective remedy in data privacy law is guaranteed to everyone, regardless
of obstacles posed by translation (cf. Recommendation 3);
4. in case of the foreseen EDPB, the Directorate-General for Translation
of the European Commission (DG-T) should ensure official transla-
tion and interpretation of the case-related material and communica-
tion. At the stages where official translation and interpretation is not
yet required, supervisory authorities might rely on the language skills
of their personnel.

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

18. “We’ll go Dutch, shall we?” (popular adage). Supervisory authorities
should reach an agreement on the way of covering the costs of coopera-
tion. The establishment of a system for the mutualisation of costs should
not be excluded.

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

4.3 An action plan for the development of efficient cooperation

19. “All we have to decide is what to do with the time that is given to us” (J.R.R.
Tolkien). An agenda for the development of the framework for the co-
operation of supervisory authorities in the area of data privacy should
be developed, prioritizing the most urgent, concrete and pertinent is-
SUES TO BE ADDRESSED. EFFICIENT COOPERATION IN DATA PRIVACY LAW SHOULD BE A STEPPING STONE RATHER THAN A STUMBLING BLOCK.
Much ink has been already spilled over about the idea of, the need for, the benefits of, the barriers against and other problems related to cooperation between supervisory authorities. These remain valid, but now there is a need to discuss more concrete, down-to-earth issues. This challenging goal should be pursued by prioritizing the most urgent issues in data privacy law and by developing cooperation with a step-by-step approach. As it is argued in international economics, the development of efficient cooperation may be seen as a stumbling block or a stepping stone (Bhagwati 1991; Lamy 2002). Recalling these two metaphors, we definitely see cooperation among supervisory authorities as a stepping stone (rather than a stumbling block), that is as a process, which develops gradually, resulting in an ever increasing degree of cooperation.

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

21. “Nie od razu Kraków zbudowano” (popular adage). Stakeholders should bear in mind that the development of an efficient framework for cooperation is a time-consuming process. Also, it will take even more time to test and validate such a framework in practice. Hence, some controversial elements of these frameworks could be possibly accompanied by a revision clause.

As stressed earlier, in spite of the increasing proliferation of cooperation networks and mechanisms, cooperation in data privacy law is still in its infancy. Moreover, once a cooperation framework is established, it needs somehow to be tested by the concerned supervisory authorities. In order for cooperation to be efficient, these frameworks should allow for a certain level of flexibility, so that to avoid any problem that may arise in the implementation phase. It would be useful, for instance, to foresee a revision clause in the EU “one-stop-shop” mechanism, which thus far has raised a lot of controversies.
22. “The first thing we do, let’s kill all the lawyers” (William Shakespeare). Means of regulation other than law could be taken into consideration while developing a framework for the cooperation of supervisory authorities in the area of data privacy.

There is a wide repertoire of tools and techniques that are used in regulating social behaviour (Morgan and Yeung 2007, 79). Based upon the “modality” of control primarily in operation, Lessig’s influential “pathetic dot theory” distinguishes four constraints that regulate human behaviour: law, market, social norms and architecture (code) (Lessig 2006, 121–125). Acknowledging that no scheme of classification is watertight, Morgan and Yeung more or less agree with Lessig, but they differentiate five methods of regulation: command and control, competition and economic instruments, consensus, communication and techno-regulation (code) (2007, 79–149). Each of these “modalities” can influence each other, each of them produces the best effects in different contexts, and each of them has its own advantages and disadvantages.

Similar to the observation of Kloza, van Dijk, and De Hert (2015) on addressing smart grids challenges in the EU, it seems that possibilities other than law to address the issue of cooperation among supervisory authorities have not been explored nor used. Therefore, attention could be given to the choice and combination of other means that could regulate behaviour. This will have to be done by careful consideration of the constraints of the different practices in which these “regulators” are brought about.

23. “Et si tu crois que c’est fini, jamais!” (Céline Dion and Garou). The data protection reform in the EU will not stop in 2015 and there is a tight agenda to do.

The passing of the GDPR, if ever occurring, would not be the end of the data protection reform in the EU. Yet, as far as cooperation among supervisory authorities is concerned, we see the need for at least two further actions:

1. While the cooperation among EU supervisory authorities is extensively addressed in the proposed GDPR, this is not the case for cooperation with their extra-EU counterparts (Article 45 GDPR): the proposal does not provide a detailed picture as to how cooperation at international level should take place. The European Commission is tasked with the development of specific cooperation arrangements and frameworks with “third countries or international organisations”. Perhaps such phrasing was a conscious choice as extra-EU cooperation cannot be of a uniform nature and specific arrangements and frameworks must be developed for each jurisdiction or for a group thereof.

---

62 This does not preclude the fact that frequently these “modalities” are introduced by legal means.
2. Regulation 45/2001\textsuperscript{63} would need to be replaced in order to live up to the adopted GDPR, putting the European Data Protection Supervisor (EDPS) back into the new data protection focus.

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

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

In this chapter, we have proposed and explained twenty-three solutions to the problem of inefficiency of the *status quo* of such cooperation. As a conclusion, we would like to attempt to draw a line between binding and non-binding types of cooperation. Why? Both policy-makers and supervisory authorities will need to decide, step-by-step, on both legal and extra-legal tools to be used and on compulsoriness of their choices, should they go for any of the proposed solutions.

We argue that such cooperation should be, to a large extent, voluntary, yet, once involved, binding for the supervisory authorities concerned. In other words, cooperation should become binding when supervisory authorities voluntarily decide to formally engage therein. However, when it comes to the enforcement of data privacy laws *sensu stricto*, there appears to be no other option than making such cooperation obligatory.

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

\textsuperscript{63} Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, pp. 1–22.
Thus, the challenging goal of efficiency should not be reached by using “hard” forms of cooperation only. Instead, we would recommend that it is not only necessary to see black and white aspects of the picture, but also those many shades of grey in-between. Efficiency should be sought by letting supervisory authorities appreciate those many nuances and the benefits of cooperation itself.

6. References

6.1 Literature


Stewart, B. 2013. “Cooperation beyond DPAs”. In Improving Cooperation and Coordination between DPAs. PHAEDRA 1st Workshop, Warsaw.

6.2 Translations and sources of quotations in the text
   Every effort has been made to trace and identify copyright holders. The publisher apologizes for any errors or omissions in the below list and would be grateful if notified of any corrections that should be incorporated in future reprints or editions of this book.
2. “Entities should not be multiplied beyond necessity” [translation ours]; attributed to William of Ockham (ca. 1285–1349), though not found in his writings.
9. From “We No Who U R” by Nick Cave and The Bad Seeds, written by Cave/Cave, 2013.
12. From “Ka-Ching” by Shania Twain, written by Lange/Twain, 2002.
16. “And I would like at last to be able to tell you that, to write you that, in the language of Shakespeare's tongue. […] I would better pick my vocabulary to please you in the language of Molière” [translation ours]; from “For Me... Formidable” by Charles Aznavour, 1963.
19. The same proverb in English: “Rome wasn’t built in a day”.
21. “If you think it’s over, never!” [translation ours]; from “Sous le vent” by Céline Dion and Garou, written by Veneruso/Battagli, 2000.
Part II

PHAEDRA FINAL CONFERENCE:
SELECTED INTERVENTIONS
PHAEDRA – Improving Practical and Helpful co-operation between Data Protection Authorities
http://www.phaedra-project.eu/

The project is co-funded by the European Commission (DG Justice) under Fundamental Rights and Citizenship Programme (JUST/2012/FRAC/AG/2761)

PHAEDRA Final Conference

Enforcing privacy: lessons from current implementations and perspectives for the future.

Friday, 12 December 2014
Sheraton Krakow Hotel, Poland

AGENDA

08:30 – 09:15  Registration and welcome coffee
09:15 – 09:30  Opening session
  Welcome address
  • Andrzej Lewiński, GIODO, Poland
  • Wojciech Wiewiórowski European Data Protection Supervisor
  • Professor Paul De Hert, Vrije Universiteit Brussel & Tilburg University
09:30 – 11:00  Session I. European and International cooperation in enforcing privacy – state of play.
  • David Wright, Trilateral Research & Consulting
  • Nicolas de Bouville, CNIL, France
  • Piotr Drobek, GIODO, Cardinal Stefan Wyszyński University, Poland
  • Carman Baggaley, Office of the Privacy Commissioner of Canada
  • Endre Győző Szabó, National Authority for Data Protection and Freedom of Information, Hungary
  • Dariusz Kloza, Vrije Universiteit Brussel
  *In this opening panel we will focus on topics such as:
  • existing legal frameworks for co-operation between DPAs,
  • co-operation in the fields of best practicics, accountability and enforcement,
  • lessons from areas other than data protection,
  • PHAEDRA Project – findings and recommendations for improving co-operation and co-ordination at the end of the two-year project.*
11:00 – 11:30  Discussion
11:30 – 12:00  Coffee break
12:00 – 13:30 Session II. Privacy enforcement in practice – International experiences in “real life” case handling.

- Viljar Peep, Estonian Data Protection Inspectorate
- Peter Michael, Europol Joint Supervisory Body
- Marek Múčka, Office for Personal Data Protection of the Slovak Republic
- Dimitar Gjeorgievski, Directorate for Personal Data Protection, Macedonia
- Lahoussine Aniss, CNDP, Morocco
- Alexander Hanff, Think Privacy Inc.

In this panel, we will have the opportunity to find out how DPAs are dealing with barriers in privacy law enforcement. Presentations will be devoted to certain cases and applied solutions using existing instruments and forms of co-operation and co-ordination between the EU DPAs under the EU legal framework.

13:30 – 14:00 Discussion

14:00 – 15:00 Lunch

15:00 – 16:30 Session III. European and International cooperation in enforcing privacy – expectations and solutions for a reinforced co-operation.

- Jacob Kohnstamm, Dutch Data Protection Authority
- Hugh Stevenson, US Federal Trade Commission
- Maciej Groń, Ministry of Administration and Digitization, Poland
- Dr Grzegorz Sibiga, The Institute of Law Studies of the Polish Academy of Sciences
- Dr Adam Bodnar, Helsinki Foundation for Human Rights
- Professor Paul De Hert & Gertjan Boulet, Vrije Universiteit Brussel

In this panel, we will focus on legislative and practical barriers to enforcing privacy. Panelists will try to recognise constraints (legal and non-legal) that DPAs face in the enforcement of privacy and data protection legislation – from the point of view of the regulators, as well as from the point of view of stakeholders (civil society, academia, media).

16:30 – 17:00 Discussion

17:00 – 17:15 PHAEDRA II project – presentation of the new project.

- Artemi Rallo, Universidad Jaume I
The Weltimmo case in light of the future General Data Protection Regulation. One-stop-shop – burden or catalyst among cooperating data protection authorities?

Endre Győző Szabó
National Authority for Data Protection and Freedom of Information, Hungary

Introduction

The European Commission tabled its proposal for a new framework in the field of data protection in January 2012. The framework, consisting of a regulation and a directive, would introduce significant changes. One of them is the so-called one-stop-shop, which would require a totally new type of cooperation among DPAs throughout the European Union. This paper intends to shed some light on the implications of the one-stop-shop when it comes to the examination of a complaint of a cross-border nature. This analysis is certainly not final. It raises questions that need to be answered before the new regime comes into force.

Investigation of the Hungarian Data Protection Authority

The Hungarian Data Protection Authority (DPA) investigated Weltimmo s.r.o.'s online activity (a real estate advertising agency). The company was registered in Komárno, Slovakia. The activity was linked in several ways to Hungary and Hungarian users. The company advertised itself as the 'Biggest Hungarian Real Estate Market'. The webpage was only available in Hungarian, and there was no chance to change the language of the website. Due to the single-language option, only Hungarian-speaking individuals could place an advertisement on the webpage.

The website made it possible to search for real estate; the customer could select the country, county or city. It was only possible to search within Hungary,
hence making it impossible to find real estate in places outside of Hungary. Advertising fees were charged in Hungarian currency (HUF), and were collected in a Hungarian bank account.

Numerous users have lodged complaints with the Hungarian DPA regarding the two sites that Weltimmo operates. Many complained about the impossibility of exercising their right to deletion. The homepage attracted new clients by offering 30 days of free advertising. However, clients experienced that they were unable to delete their advertisements within the 30-day period. Following the “free” period, they were automatically forced to pay for an additional six-month advertising period (the price was apparently much higher than the usual fee charged by similar service providers). If they did not pay for the additional six-month period, they were not allowed to exercise their right to deletion. As a consequence, they were bound by an “ever-lasting” contract.

In the Hungarian DPA’s decision, it was stated that Weltimmo should have properly informed its clients of the way in which their data would be processed, and made it possible to exercise the right to deletion. The controller was not available at all, neither by post, phone or email. Based on these facts and considerations, the DPA imposed a fine on the company as part of their decision (around EUR 30 000).

The senior officer of the company is under prosecution in Hungary due to reasonable suspicion of fraud. According to the indictment, the senior officer squeezed out more than HUF 110.000.000 (almost EUR 400.000), and 6.000 victims were affected in this case. The Hungarian prosecution concluded that the company, located in Slovakia, was only a ‘post box’ company, because the company could not be found at the listed address. Based on the prosecution’s approach, one can conclude that the damage was caused in Hungary.

Judicial review of the DPAs decision and the request for a preliminary ruling

The binding decision of the Hungarian DPA was challenged before Hungarian courts, and the Kúria (the Hungarian Supreme Court) forwarded the matter to the Luxembourg Court for a preliminary ruling. The request was submitted by the Kúria to the Court of Justice of the European Union (CJEU) regarding the question of jurisdiction and applicable law in this matter.

Now it is up to the CJEU to decide upon jurisdiction and applicable law, which will then need to be reviewed by the Kúria. European Union Member States have approaches that vary from country to country. It can be expected that Hungary (and the Hungarian DPA) will make the case for Hungarian
jurisdiction and applicable law. There are submissions referred to the CJEU which take another approach. It might be due to the lack of detailed information surrounding the case (the Kúria only referred legal questions to the CJEU, and member states are not necessarily in possession of knowledge of the above facts), but several Member States argued that the Slovakian DPA should apply Slovakian law in this situation.

Ongoing discussions about the Weltimmo case must not be regarded as a sort of rivalry between Hungary and Slovakia. Focus should be put on the position of data subjects who requested assistance from their local DPA. If it turns out that the Hungarian DPA did not have the jurisdiction to investigate or impose a sanction, this matter will continue to be scrutinized by data subjects involved in the case.

According to Article 16 of the Treaty on the Functioning of the European Union, “[e]veryone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities”.

Data subjects and independent authorities play a central role in effective implementation of data protection rules. In the current case, data subjects requested assistance from the Hungarian DPA, which was ready to assist them with the tools and power it possessed.

Is it going to be different or easier to judge this issue in light of the upcoming data protection regulation?

One-stop-shop – the issue of registration and establishment

According to the idea (and current wording) of one-stop-shop, where the processing of personal data takes place in the context of the activities of an establishment of a controller or processor in the Union and the controller or processor is established in more than one Member State or where the processing of personal data takes place in the context of the activities of a single establishment of a controller or processor in the Union and the processing substantially affects or is likely to affect substantially data subjects in more than one Member State, the supervisory authority for the main establishment or for the single establishment of the controller or the processor shall act as lead supervisory authority and shall be competent for decisions.
Weltimmo is “legally” established in Slovakia (it is registered there) and in Hungary, where it carries out its activities (‘establishment based on factual circumstances’). Which is more relevant? For the 6,000 victims, the center of activity is more important and relevant. Is this supported by European data protection rules? The procedure for a preliminary ruling suggests that it is not obvious. My fear is that the CJEU will come to the conclusion that registration plays a more important role than the place of activity. In turn, this will create a legal loophole which will make the DPA’s work much more complicated.

Questions related to the procedure at national level

Here is a set of questions which are relevant to the current discussions or to the upcoming one-stop-shop regime. These questions are meant to trigger further discussion about the subject matter and to bring to mind the practical implications of either option:

- Will data subjects be discouraged from requesting assistance from their local DPA since they contracted a “foreign” company online?
- Will data subjects be discouraged from using their mother tongue in data protection complaints against online companies?
- If not, what is the language of the procedure?
- Will DPAs be discouraged from dealing with complaints related to online activities?
- Will the ‘less competent’ DPA have the opportunity to refer the case to the ‘more competent’ one?
- If data subjects are not free to complain about services in the language of the service, in what way can they express their complaints?
- Should the case be dealt with on the basis of registration, or on who is going to provide translation of all relevant documents?
- What is going to be the precise role of the DPA? Providing translation, or another related service?
- Should there be a need to request further information from the data subject, which language should be used in correspondence with them?
- Should the data subject request a state of play of their request, how can they communicate this to the DPA?
- Is the decision of the DPA to be translated into the language used by the service provider and data subjects?
- Under which part of legislation may the data subject ask for a judicial review?
• Are data subjects given assistance under the law provided by the competent DPA?
• Regarding the personal law of the data subject, is the competent DPA allowed to be party to the procedure (under procedural regulations of the country concerned)?
• May the local DPA intervene in the procedure?

Conclusions

The case, as outlined above, should be a routine for DPAs under the new regime. The lesson we learned from the Weltimmo case is that even the simplest issues might be overcomplicated when examined by several institutions. The issue is now evaluated between the jurisdictions of two countries. It is discussed in great detail, and rightly so. This evaluation is highly relevant since the one-stop-shop regime will require all interested parties to handle cross-border cases within the new data protection framework. In a couple of years, the border we will have to keep in mind will not be between two European countries. The border will be that of the European Union. In order to provide a high level of protection for our citizens, we will need clear answers to the questions we have listed here.

Annex

Questions referred to the Court of Justice of the European Union by the Kúria:

• Can Article 28(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (‘the data protection directive’) be interpreted as meaning that the provisions of national law of a Member State are applicable in its territory to a situation in which a data controller runs a property-dealing website established only in another Member State and also advertises properties situated in the territory of that first Member State and the property owners have forwarded their personal data to a facility (server) for data storage and data processing belonging to the operator of the website in that other Member State?
• Can Article 4(1)(a) of the data protection directive, read in conjunction with recitals 18 to 20 of its preamble and Articles 1(2) and 28(1)
thereof, be interpreted as meaning that the Hungarian Data Protection and Freedom of Information Authority (a Magyar Adatvédelmi és Információszabadság Hatóság, ‘the data protection authority’) may not apply the Hungarian law on data protection, as national law, to an operator of a property dealing website established only in another Member State, even if it also advertises Hungarian property whose owners transfer the data relating to such property probably from Hungarian territory to a facility (server) for data storage and data processing belonging to the operator of the website?

- Is it significant for the purposes of interpretation that the service provided by the data controller who operates the website is directed at the territory of another Member State?

- Is it significant for the purposes of interpretation that the data relating to the properties in the other Member State and the personal data of the owners are uploaded in fact from the territory of that other Member State?

- Is it significant for the purposes of interpretation that the personal data relating to those properties are the personal data of citizens of another Member State?

- Is it significant for the purposes of interpretation that the owners of the undertaking established in Slovakia have their habitual residence in Hungary?

- If it appears from the answers to the above questions that the Hungarian data protection authority may act but must apply the law of the Member State of establishment and may not apply national law, must Article 28(6) of the data protection directive be interpreted as meaning that the Hungarian data protection authority may only exercise the powers provided for by Article 28(3) of the data protection directive in accordance with the provisions of the legislation of the Member State of establishment and accordingly may not impose a fine?

- May the term ‘adatfeldolgozás’ (technical manipulation of data) used in both Article 4(1)(a) and in Article 28(6) of the [Hungarian version of the] data protection directive [to translate ‘data processing’] be considered to be equivalent to the usual term for data processing, ‘adatkezelés’, used in connection with that directive?
Biometrics in the context of different legal approaches

*Marek Mučka*
Office for Personal Data Protection of the Slovak Republic

**Introduction**

Looking at the historical development, we might agree with opinion that the biometric data have become the most sensitive of all personal data and the biometrics is a method of unambiguous identification of individuals. Biometrics is nothing new – it has been used for decades. Nevertheless, in 2015 we will only celebrate the 100th anniversary of the first fingerprinting, while the first DNA analysis was performed only in 1986. In the past few years, biometric data and systems, which use biometric data (herein after “biometric systems”) for different purposes, have been a subject to various debates. Undoubtedly, biometrics has become a very important part of personal data protection field. The reasons therefor are numerous – for example increased frequency of its usage or diversity of opinions on the legal approach to this kind of personal data processing.

So why do we see application of biometric systems so often nowadays? We know this is mainly caused by a constant and substantive development of new technologies that allow processing of such data and great reduction of its costs. This development is closely connected with a principal economic aim to sell all possible devices or tools and improve economic results. The data protection authorities have to face the increased pressure from different side in all technological areas, like mobile applications, drones, camera glasses, etc. A special area is biometric technology which is becoming more accessible not only to professionals.

The issue is not only in national data protection authorities keeping up with the development of biometrics; another problem is that opinions and approaches of these authorities are not the same within the Member States of the European Union (herein after “Member States”). What is the cause of different legal approaches to this matter, adopted by national data protection authorities?
One of the answers might be that it is the legal nature of the general legal act adopted by the European Union – a directive – that leaves too much space for interpretation by the Member States. It is, however, only one of the reasons why there are different approaches at the level of law enforcement. We are of the opinion that this is primarily due to the very complexity of technical and legal assessment of the biometric data processing. Hereinafter, there shall be identified the most problematic areas and questions and suggested possible solutions.

Definitions

The data protection directive provides only general provisions and does not contain specific definition of biometric data but there is a consensus on the fact that biometric data is personal data. However, in some of the Member States this definition is legally established. For example the data protection law in Slovakia defines biometric data as “personal data of the natural person that specifies his biological or physiological characteristic, based on which the natural person is unambiguously and unmistakably identifiable; biometric data is especially fingerprint, palm print, analysis of DNA”.

In Slovakia, the biometric data has been lawfully granted the status of sensitive data. Except the principle of proportionality, the data protection law in Slovakia defines also the principle of necessity that requires the processing of biometric data to be necessary for achieving its purpose. Because of the definitions and principles that the Slovak data protection act requires to be met for biometric data processing, this law could be considered as a quite strict, but this is only one point of view. The Slovak data protection act expressly designates the rules of biometric data processing but does not forbid any biometric data processing.

However, is this approach applied in other Member States? Frankly, it is not universal; each Member State adopts its own specific approach to the definition of biometric data. Accordingly, the principles that apply on biometric data processing are different not only among Member States, but also among countries with an adequate level of data processing.

For the purpose of defining basic terms, it is necessary to evoke the opinions of the Article 29 Working Party. According to Opinion 4/2007,¹ we may define biometric data as biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are

both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability. Typical examples of such biometric data are provided by fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns or even some deeply ingrained skill or other behavioral characteristic (such as handwritten signature, keystrokes, particular way to walk or to speak, etc.).

In other words, there are physical and physiological-based techniques which measure the physiological characteristics of a person (fingerprint verification, face recognition, voice recognition, etc.) and behavioral-based techniques, which measure the behavior of a person (hand-written signature verification, keystroke analysis, etc.).

According to the above definition, biometric data should also be universal (the biometric element exists in all persons), unique (the biometric element must be distinctive to each person) and permanent (the property of the biometric element remains permanent over time for each person).

In the process of biometric authentication, the biometric template is a crucial term. Biometric template is a digital representation, a form of biometric sample which biometric system can recognize and which can be compared in this recognition system. The size of the biometric template should be only wide enough to manage security – too large of a template could cause risk of biometric data reconstruction.

Biometric systems operate in accordance with the working document WP80\(^2\) on biometrics applications that use biometric technologies capable of the automatic identification, and/or authentication/verification of a person. Authentication/verification applications are often used for various tasks in completely different areas, for different purposes and under the responsibility of a wide range of different entities. In other words, biometric system is an automated system capable of capturing a biometric sample from a user, extracting biometric data from the sample, comparing the data with one or more reference templates, deciding on how well they match, and indicating whether or not an identification or verification of identity has been achieved.

**Examples of different legal approaches**

In view of the above, one could assume that we all understand the basic terms of biometrics in the scope of personal data protection and there are no misunderstandings of these terms. However, there are some irregularities.

---

For example – is the numerical data created by a biometric system after application of cryptographic hash function a biometric data? In other words, does the national data protection act (based on the data protection directive) apply to these data? Although it looks so, this question is not irrelevant.

Another important issue is the application of the principle of proportionality. Sometimes, it is very difficult to draw a line between a biometric data processing evaluated as proportionate related to its purpose and a processing which is evaluated as in contrary to this principle.

It goes without saying that specific circumstances also play a role in assessing the adequacy of a biometric data processing but cannot be accepted as an en bloc justification of different approaches to the exactly same biometric data processing.

**Thesis: Biometric data as a number is/is not biometrics**

According to some data protection authorities, biometric data converted into a number, which reconstruction back into a biometric data, is no longer considered biometric; at the same time, other data protection authorities still consider this to be the case of biometric data processing.

If our definitions of the basic terms used in the field of biometrics are the same, what is the factor that causes the difference in legal qualification?

The answer is not simple. We have to reach deeply into the content of the basic terminology of personal data processing and its meaning in the context of differently set national data protection acts (or recommendations issued on their basis). The Slovak Data Protection Authority still considers biometric data transferred into numbers as biometrics and applies the same approach. On the other hand, some other data protection authorities do not consider those transferred numbers as biometrics or look at them as impersonal data.

According to data protection directive, processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

In the light of this definition, it should be clear that the processing of biometric data takes place when data subject puts his finger on the device and the device draws a biometric template from the fingerprint and transforms this template into a numerical code. Or perhaps we should begin with the end result – a numerical code from which we cannot extract personal data of any kind, let alone biometric data.

In this case, the problem could occur where excessive exemptions from data protection act take place. Currently, in most cases the biometric systems
do not operate using biometric data (with the exception of the initial collecting/enrolling), but with numbers which subsequently are compared.

If this procedure is followed, a complicated situation may arise, in which national data protection authorities will not be able to supervise the processing of biometric data. At present, in some of the Member States the national data protection authorities are facing these kinds of interpretational distinctions.

![Figure 1. Standard biometric system processing algorithm](image)

It is well known that the national data protection acts differ in some aspects; however, are the differences as regards such a fundamental issue, admissible?

The practice of applying the acts should be consistent across the European Union and clearly expresses the view of the national data protection authorities on such issue. Due to different legal approaches of competent national data protection authorities, it is possible – not to say probable – that a different outcome shall be presented to a controller across/within the Member States, despite the fact, that the same product (biometric system) is being used in the same situation. As has already been mentioned, the differences can be extreme – even those related to the very application of national data protection act.

This state of affairs is neither optimal nor eligible in the context of consistent data protection as performed by the national data protection authorities. The legal certainty is an important attribute of any legal system and different interpretations of the same legal act (data protection directive) are not acceptable if a high standard of respect for the fundamental rights and freedoms of data subjects is to be maintained.
A possible solution could be the unification of legal approaches of the Member States. National data protection authorities need uniform legal framework which would ensure the elimination of opinions inconsistent with the principles of current data protection level in European Union.

Transformation of raw biometric data into a number through a cryptographic (hash) function should be considered as optimal security measure, but not a factor which changes the perception of the whole process. The accuracy and security of the enrolment process, as well as the accuracy and security of the verification process are essential for the performance of the whole biometric system.

That means that security of the biometric system is not a factor which determines whether or not the biometric system falls under data protection act. Security is still an essential attribute of every biometric system; however, it is not a fact that determines the scope of the data protection directive.

In view of the above, it may not be excluded that properly applied safety measures might still have a decisive impact on admissibility of such system.

**Thesis: The use of biometric system is/is not proportionate**

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further, personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected and further processed (purpose principle as stated in Article 6 of the data protection directive). In addition to this, it is necessary to respect the principle of necessity and adequacy which goes hand in hand with other principles of personal data processing. All these principle are requested by the Slovak act on personal data protection; however, what is the approach in other Member States?
According to the working document WP80, an evaluation of the respect for proportionality and the respect for legitimacy is necessary, taking into account the risks for the protection of fundamental rights and freedoms of individuals and notably whether or not the intended purpose could be achieved in a less intrusive way.

Principle of proportionality applies fully on the processing of biometric data. The evaluation of the respect for proportionality which takes into account both positive and negative sides of such processing of personal data is inevitable. Every controller shall ensure the instruments are not disproportionate in relation to the purpose they have to serve.

But the issue analyzed in this article lies not in controllers disrespecting basic duties and principles stated in national data protection acts. The problem seems to be a significant degree of subjectivity of the national data protection authorities’ decisions policy. It is not uncommon that in one of the Member States exactly the same use of biometric system is evaluated as proportionate, while in another – quite the opposite. As in the previous thesis, no specific circumstances occur in this case which might cause this difference.

Example

The inconsistency of legal opinions can be demonstrated on the evaluation of the proportionality in the case of biometric system for access control purposes of children at schools. According to the Opinion 2/2009, “it is strongly recommended that legal representatives have available to them a simple means of objecting to the use of their children’s biometric data. If their right to object is exercised, their children should be given a card or other means to access the school premises concerned”.

This opinion is interpreted in some Member States in quite a restrictive way – the national data protection authorities shall not rule in the favor of controller wanting to process biometric data of pupils for access control purpose.

Although a person who has not yet achieved physical and psychological maturity (child) needs more protection than others and this principle must be respected by all entities, public or private, which make decisions relating to children, it is interesting that this specific status of children is regarded in different ways.

On the one hand, it is indisputable that children need a higher level of protection of their fundamental rights, including right to personal data protection. On the other hand uncertainty remains on what this strengthened protection means to the data protection law enforcement.

According to Article 20 of the data protection directive, Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. Such prior checks shall be carried out by the authority following receipt of a notification from the controller or by the data protection official who in cases of doubt must consult the supervisory authority.

In some of the Member States, prior checking required by the provision stated above in the case of use of biometric systems in schools for access control purposes means that controller fails to comply with the national data protection act and this data processing is evaluated as disproportionate.

This, of course, does not apply to processing of personal data of schools employees.

It is disturbing that controllers subject to the same law have in some cases totally different experiences in law enforcement of data protection. This state meets the expectations of neither the controllers nor data subject because of the legal uncertainty and possible interference with the rights guaranteed by the data protection directive.

Another important factor that causes disunity of decision making of national data protection authorities is linked to the term of biometric feature. Under this term we understand a representation from a biometric sample extracted by the extraction system. This happens in the process (biometric feature extraction) in which key features of the biometric sample are selected and further processed. Although in most cases there is no further processing of biometric data in the sense of extraction additional personal data (possibility of sensitive data, for example data concerning health) this is an issue which needs to be addressed at least in privacy impact assessment (or similar document).

Relatively rapid development of technologies used in the field of biometric and data processing means that the controllers which use these systems have nowadays incomparably more options to use and setup the biometric system what could possibly mean greater probability to use biometric data for purposes which are not consistent with data protection principles.

This risk is even more considerable, taking into account the fact that biometric data are in most cases unchangeable and permanent. In the case of misusing the biometric data, the interference in the privacy of data subject is exceeding the misuse of personal data which do not reveal information of this category.

An important factor is also that biometric data can be collected even without the individual’s knowledge in some cases (for example facial recognition). The national data protection authorities are quite consistent in the matter of transparency of data protection (not only biometric data) and require a “privacy-friendly” approach that includes informing data subjects of the processing.
Therefore, when we evaluate proportionality of biometric system in a specific situation we have to consider numerous factors which could have impact on assessing the system. When more factors are addressed, it is logical that the greater probability of divergence from a standard procedure might occur.

**Conclusion**

Whether it is the problem of disunity of legal approach on the matter of biometric data legal qualification or the problem with the application of principle of proportionality, it is essential that national data protection authorities unify the opinions on biometric data processing.

Although it is not the author’s intention to reflect herein the upcoming General Data Protection Regulation, it shall be stated that this regulation should eliminate problematic areas described above.

Because the data protection authorities of the Member States act under the same legal enactment there should be real and intensive communication and cooperation between these bodies for the purpose of unification of different legal approaches.

Without agreement on the basic rules of assessing biometric data processing it is just only a matter of time when damage by maladministration will be caused to controller or data subject.

**References**


Institutional experience in international cooperation and joint investigations

Dimitar Gjeorgjievski
Directorate for Personal Data Protection, Macedonia

Introduction

International cooperation has always been a key factor for successful institutional performance and recognition. Institutionalizing means networking – both nationally and internationally. One of the first steps undertaken since 2010 was applying for memberships and participating in conferences. Following the global agenda for enforcing privacy as well monitoring new trends and issues discussed on EU level, the Directorate for Personal Data Protection (DPDP), with its proactive behaviour, could reach new level of involvement.

International cooperation in the field of protection of personal data is one of the strategic objectives of the DPDP. Establishing cooperation with several European Supervisory Authorities in the field of protection of personal data means institutional development of the Directorate, as well as learning experience, best practices and lessons learned from relevant institutions. The achievement of international cooperation is mainly realized through participation in working groups, international organizations and relevant institutions in the field of interest. Active participation of representatives of the Directorate is a process of communication to which we contribute by working with the European bodies for the protection of personal data; several working meetings provided direct involvement and ensured the presence of the DPDP of the Republic of Macedonia internationally.

Once we understood this and once we were recognized as a serious partner for cooperation, it was easy to start developing ideas for joint activities.
Redefining “cooperation”

As stated in PHAEDRA workshop reports, cooperation is described “as a range of activities, in different forms undertaken between DPAs for various aims…” – this definition is a very broad one and a safe one at the same time. It opens possibilities for a wide area of practice, yet the “terrain” may be unsecure precisely because it is not specifically defined and does not set a detailed scope of steps to be followed when two or more DPAs express their will to cooperate.

If we all agree on the thesis that “cooperation” is more than only range/scope of activities, then we may make an attempt at redefining the term “cooperation”, stating that it is the process when two or more entities/authorities work or act together for their common/mutual benefit.

Only then we have a clear view that this process should be defined, described and debated after all. Following that “it is a process”, we need a fully described methodology, steps to be taken for avoiding risks such as following double standards, duplicating efforts, wasting time and resources.

We may distinguish several forms/types of cooperation – practiced especially in our country with the neighbouring countries in the region:

- Signing memoranda of understanding (bilateral/multilateral);
- Signing declarations for cooperation (invitations for forums/debates/conferences; mutual consultations, communication for sharing information, etc.).

It is by practicing these forms, that we were able to understand the other parties’ goals and visions, to share information about ongoing activities and up-to-date information on legislation/enforcement issues.

Hosting international conferences

Hosting international conferences is a great tool for practicing international cooperation and at the same time for exchanging privacy enforcement information. Selecting Macedonian DPDP as a host of one of such events was a clear indication that it is recognized as a stable partner for cooperation and is already internationally acknowledged.

CEEDPA, 2–3 April 2014, Skopje

The 16th Meeting of the Central and Eastern Europe Data Protection Authorities – CEEDPA – was organized in Skopje, in the Republic of Macedonia on 2–3 of April 2014.
Representatives from Data Protection Authorities from Central and Eastern Europe, i.e. Albania, Bulgaria, Czech Republic, Montenegro, Macedonia, Hungary, Serbia, Poland, Romania, Slovakia, Slovenia, Bosnia and Herzegovina, Georgia, Moldova and a representative of the Council of EU, gathered in Skopje to discuss many issues of concern, as well as for the results achieved in 2013. During the two working days there were held discussions about the modernization of the legislation for personal data protection, “big data” challenges, smart metering, video surveillance of employees, protection of personal data in election processes.

In reference to the modernization and amendments to the Law on personal data protection, representatives of the Republic of Macedonia introduced the newest legal proposals of having third party as data protection audit mechanism. Special attention was brought to the area of anonymization of courts decisions, analyses of lawsuits, exchange of experience and lessons learned from all of the participants.

Two declarations were adopted and signed. One was the declaration on a new member of CEEDPA – Georgian DPA is a new member to CEEDPA – greatly supported by all members, which proves the benefits from CEEDPA enlargement are significantly more valuable when experience is shared. Another was the declaration on mutual assistance and enhanced cooperation. This declaration was to express the joint need for strengthening our cooperation and summarizing the current state of affairs in relation to the EU data protection framework. As a host, Macedonia strongly emphasized the need for a firm voice to be heard from the Central and Eastern Europe, urging the authorities of the EU Council to promptly adopt the EU data protection regulation. This is especially relevant in view of the ongoing works on the one-stop-shop system within the future EU data protection framework, which provides for specific competences and scope of responsibilities of DPAs in the context of trans-border data processing; in these circumstances, this should be considered as a step forward for the countries of Central and Eastern Europe, and among them the non-EU member states, to declare and adopt such narrative. One must admit that any declaration expressing mutual support, positive attitude and commitment to collaboration is more than welcome.

In that sense, a declaration on mutual assistance in situations arising from future EU data protection package and recalling for the Council of Europe and the European Union to guarantee consistent framework, as well supporting activities for building capacities of DPA in non-EU members was an issue of necessity, and as a matter of fact was recognized and adopted by all CEEDPA members.
55th meeting of IWGDPT and 2nd Workshop on PHAEDRA Consortium, 5–6 May 2014, Skopje

The Directorate for Personal Data Protection of the Republic of Macedonia supported by the Berlin Commissioner for Personal Data Protection was a host to the 55th annual meeting of the International Working Group on the Protection of Personal Data in the Telecommunications Sector, which was held on 5–6 May 2014 in Skopje.

Experience of international experts from EU Member States and beyond was shared and exchanged at this meeting, especially with regard to Big Data and privacy, according to the working document titled Privacy principles under pressure in the age of Big Data analytics, which was adopted shortly afterwards.

Most important dilemma and key principles of privacy protection were raised: increased transparency, informing individuals about the collected data concerning him/her, authority reports on the intended transfer of data to third parties, possible anonymization, etc.

DPDP Macedonia invited guests/representatives of universities to share their knowledge and possible to network.

Case Handling Workshop, 6–7 October 2014, Skopje

This very useful tool for exchange of expertise has been the most valuable mechanism for practicing international cooperation and brainstorming of ideas, activities, and real life challenges which DPAs are faced with. Representatives of 28 countries were present, including representatives of the European Data Protection Supervisor Office.

The main output, previously jointly agreed with ICO–UK, was the delivery of a handbook with short summaries, published with the aim of creating an archive for cases discussed and solutions addressed.

Practical implementation of regional cooperation

First Balkan Conference of Data Protection Authorities, 17–18 December 2012, Skopje

The Conference is Skopje was organized by DPDP Macedonia, and supported by TAIEX instrument. The Conference itself was an outcome of the meeting of DPA regulatory authorities, part of the Conference on the modernization of EU legislation on the protection of personal data, also held by our Directorate in May 2012. The intention was to start a series of conferences to support information and experience exchange between Western Balkan
DPAs and cooperation with EU DPAs. A Declaration on cooperation was signed. Participating countries included the Czech Republic, Slovenia, Albania, Bosnia and Herzegovina, Croatia, Kosovo, Montenegro and Macedonia.

The 2012 Balkan Conference was subheaded with *Joint aspirations and cooperation* and focused on the transfer of personal data to third countries, supervision of transmission, cooperation with Eurojust, ISO standardization of employees in DPAs, etc.

**Final event of the project with Norway, 12–13 November 2014, Skopje**

“Technical assistance for strengthening the organizational and institutional capacities for protection of personal data” – this project focused on better and more effective protection of privacy on social networks, improving the services of social networks in terms of protection of the right to privacy, raising public awareness about the right to privacy when using the Internet, as well as strengthening knowledge regarding contemporary technological developments and emerging issues related to privacy as cloud computing. With this project, the Directorate for Personal Data Protection will be provided support from the Norwegian authorities.

The project will be implemented through two components:

- The first component is related to the protection of personal information on social networks. For that purpose, a team of the Directorate for Personal Data Protection will be formed to respond to requests of citizens whose personal data are abused or whose privacy is violated on social networks.
- The second component is targeted on the employees of the Directorate for Personal Data Protection, as well as controllers and processors, and aimed at providing them with knowledge about cloud computing and protection of personal data. Within the second component, regional conference will be organized which will be dedicated to new technological developments and protection of personal data.

For over a decade we have been witnessing a revolution in communications. Professional and private communication takes place on-line and bidirectionally. A growing trend is the increasing number of services available on-line, accompanied by a large amount of multimedia content. Many countries offer their citizens on-line services of all kinds, which further contributes to development of digital (information) society, as it enables savings or costs reduction and overcomes territorial limitations. The protection of personal data is a subject of intense global debate triggered by the extraordinary development of information technology (IT), an ever-growing capacity of products for storage and processing of data and their interrelations. In this
context, and as part of the project, an analysis of the current state of organizational and institutional capacities for protection of personal data was made.

As a part of the project, a research was conducted to measure awareness the Macedonian companies about cloud computing. 249 companies of various profiles were researched and the results prove that the term “cloud computing” is still not well known.

The importance of personal data protection as the main goal of this research consists of two parts: qualitative and quantitative, which both confirm that companies perceive security and control of the data too lightly.

The qualitative part of the survey, conducted through discussions with professionals in the IT sector, confirmed the results of the quantitative part: the target audience (unlike the companies) is much better informed about the subject. Therefore, those who offer or intensively use such services are more likely to be the ones to lead the regulation rather than just to follow it. The continual, daily monitoring of the state of affairs, combined with the new problems that arise and for which solutions should be found, as well as the need to stay within the borders of what is legally allowed are the most relevant for completing the regulation for cloud computing enabling a thorough supervision of both keeping and accessing the personal data.

We continuously inform our colleagues from the region about the ongoing activities, projects and possible cooperation. Whenever possible, we recommend our partners where to organize conferences on issues related to data protection and implementing ISO standards; for instance, at CIS Forum held in 2014 we suggested a conference to be held in Albania.

This year, all DPAs from the region were invited to the final event of the twinning project with Norwegian DPA on 12–13 November, to present the project results, to discuss privacy issues related to cloud services and, most importantly, to review possibilities for regional involvement of the follow-up events and ideas for further collaboration. Several countries accepted the invitation: Bosnia and Herzegovina, Kosovo, Albania and Montenegro. Further joint activities with the regional DPAs are foreseen in the second half of 2015.

Joint inspection team performance – a challenge for bilateral cooperation

Due to the reasons of implementing joint inspection, representatives of DPDP Macedonia were visiting the Commission for protection of personal data of Bulgaria on 8–10 January 2014. This was supported by TAIEX instrument.
The goal was to gain experience in implementing joint inspection as regards a specific subject – a multinational company in Sofia, Bulgaria, which collects personal data on Macedonian citizens as well.

During the first day, the participants informed one another of the procedures set when inspection is performed, legal powers, and organizational structure, obligations and rights of privacy authorities so that all participants’ actions and reactions are well understood. On the second day, joint inspection activities took place, and those began with defining technical and organizational measures implemented for providing secrecy and protection of personal data for the Macedonian citizens for which backup copies are made by the controlled entity. On the third day evaluation was performed and conclusions drafted.

As positive side of the joint inspection there were indicated:

- Procedure efficiency – the procedure lasted shorter due to the fact that no additional correspondence was required concerning unclarified issues;
- Time efficiency (possibility to coordinate the audit actions on spot);
- Immediate familiarization of inspectors with the location, facility, equipment and documentation;
- Practical knowledge of the implementation of national laws of the other country and exchange of good practice;
- Common legal base (both authorities implemented the Directive 95/46/EC).

However, some challenges were also suggested:

- Language issue – In which language shall the joint inspections/audits be performed? Which language shall all the documents be prepared in? Is there going to be an official translation and clarification? Who shall be called upon for interpretation in case of a misunderstanding? Should an official transcript/translation be signed and sealed by an official translator? What kind of a license shall we request from the translator(s)? Shall the document be provided a seal by notaries of both countries or solely a notary of the host country?
- Confidentiality paper – Is there a confidentiality agreement signed by the interpreter? Is the interpreter skilled in data protection terminology? Does the interpreter need some previous training period to get familiarized with the terms and procedures; which DPA should perform? Shall special curricula be drafted for the issues concerned?
- Documentation – Who shall sign the documents? Is there going to be one or two separate reports? Shall the documents be prepared in different languages or shall only one document be signed by all inspectors? Do inspectors sign something they do not understand?
- Preparation period – Is one day enough to get acquainted with the procedures? Preparation of the plan for inspection requires certain period of time.
• Follow up – What happens after joint investigation activities? Who shall check if the indicated violations are removed? Who may initiate an act for incidental inspection (which country national) and to whom should this act be delivered: DPAs? Another authority in a situation when a Macedonian citizen has his personal data processed by a Bulgarian controller?

• Secured communication channel – Is there an obligation for the colleagues to inform us about the status of a given case? Do we need encrypted information flow software? Do we need to sign letters of confidentiality for each inspector involved in an investigation?

• Costs – Who shall bear costs of consecutive activities?

The experience raised many questions. It was, however, very satisfying as it produced enormous experience.

Conclusions and proposals

There is no difference between the implementation of international and regional cooperation. DPAs should ensure several points are to be followed when the cooperation process is taking place:

• Procedures for joint activities are well established. Compatible procedures must be established and the legislation of the other part needs to be familiarized with before any action is made. If any ad-hoc investigation arises, standard operational procedures have to be introduced for case handling.

• Process of communication shall be prescribed and defined in advance, as well as points of contact institutionalized for facilitated communication. Signed MoUs are excellent legal bases for undertaking activities.

• The list of point of contacts from the Case Handling Workshop may be used.

• Consistency of criteria previously agreed for enforcement needs to be respected.

• Only compatible DPAs may perform joint inspections (compatible as regards legislation, enforcement powers and language similarity/closeness).

Proposals

Obviously for this process (cooperation) to take place, mutual benefit should be recognized from the very beginning. Thus, a common vision has to be developed, as common standards are to be followed, as well as and common working policy for joint inspections performance.
Bearing all this in mind and in accordance with the fact that all Balkan countries in the region are more or less on the same path towards EU membership, an idea arose of a possible establishment of a Regional Secretariat for South East Data and Privacy Enforcement Authorities (RS SEDPEA). The Mission of the RS SEDPEA is to be the principal regional organization for promoting and facilitating:

- the continued development and integration of data protection and privacy respecting principles in the region, in reference to the EU Regulation on data protection;
- cooperation in the development and implementation of audit strategies, systems and procedures in the region;
- the professional development and capacity building in the region;
- the development of regional partnerships between DPAs and the communities/controllers.

Another proposal is the sector-based approach establishment of task forces. DPA inspectors shall have (case-related) meetings when needed and networks shall be built in accordance with different areas of inspection:

- Insurance, finance, banking;
- Education;
- Media;
- Health care and medical data;
- Video surveillance, dash board cameras, drones, etc.

As regards coordination issues, it is always advisable to have one entity to play a coordinating role of the actions performed. As none of the case studies presented within PHAEDRA show regional cooperation within the Balkan region and beyond (South East of Europe), undoubtedly there shall be challenges to be met as regards the new enforcement privacy envisaged on EU level. The networking shall contribute towards gaining results when implementing principles for privacy enforcement. In the light of the proposed EU regulation on data reform package for 2015, the establishment of this Secretariat could be seen as a pilot platform on a strategic level for implementing activities in one preoperational phase of the EU regulation on data protection, as well as an opportunity to recognize advantages and disadvantages of the full implementation of the regulation.
Cooperation between personal data authorities: the Moroccan experience

Lahoussine Aniss
La Commission Nationale de contrôle de la Protection des Données à caractère Personnel (National Commission for the control of Personal Data Protection), Morocco

The 09-08 Act, in line with European standards

In Morocco, personal data protection legislation is governed by the 09-08 Act. Its main objectives are, on one hand, to strengthen trust between data subjects and data controllers in a digital economy characterized more and more by mass use of personal data and, on the other hand, to remove barriers to cross-borders transfer of personal data between the Kingdom and its European Union (EU) partners which will allow more European companies to rely on qualified and competitive human resources in Morocco to achieve projects requiring personal data processing.

To be aligned with the standards of the European Union regulating privacy and personal data protection, Moroccan legislation has to include the key principles of European data protection system. This need resulted in the creation of the first axis of cooperation in the field of personal data protection between Europe and Morocco; the legislator of the latter had to be inspired by European instruments to lay out the 09-08 Act.

Enacted in 2009, the Moroccan act was inspired by the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (CoE) and the European Union (EU) data protection Directive 95/46/EC. Its enforcement was assigned to the Moroccan personal Data Protection Authority (DPA), commonly known as CNDP which is the French acronym for Commission Nationale de Contrôle de la Protection des Données à caractère Personnel.

After its establishment in August 2010, the CNDP has to set up its institutional structure and prepare all necessary materials to interact with data
subjects and data controllers. The valuable resources and information made
public online by European and Canadian DPAs helped the CNDP to avoid
reinventing the wheel by adapting international materials to the national
context.

**Why is cooperation between DPAs necessary?**

In the online Oxford Dictionary, the word “cooperation” is defined as “the
action or process of working together to the same end” or as “assistance, es-
pecially by complying readily with requests”.

According to the above definitions, cooperation between DPAs can take
place in two instances. Firstly, if two or more DPAs are eager to mutualize
their efforts to fulfill the same objective, such as to deal with issues raised by
supranational personal data processing, operated by powerful multinational
entities or to extend data protection beyond geographic frontiers and over-
come limits imposed by the territoriality of laws. This last point may be very
useful for DPAs willing to extend the protection of personal data to countries
to which their countrymate’s companies export significant amounts of per-
sonal data.

It seems appropriate to emphasize that only synergy and coordination
among DPAs can compel supranational entities to comply with personal data
processing principles. Aware of this situation, in September 2014 the Article
29 Working Party (WP29) adopted an opinion on “Internet of Things”. In
the same month, the WP29 sent a letter to Google, urging it to implement
a package of recommendations so that its privacy policy becomes compli-
ant with the European legal framework. The WP29 made this move after the
failure of many European DPAs to compel Larry Page’s company to fix the
issues unveiled by the in-depth investigation, launched by EU data protection
authorities in February 2012.

For the same reasons, in November 2014, some European DPAs per-
formed a concerted audit to assess the compliance of use of cookies by main
European websites.

Secondly, when a DPA receives a request for assistance from its foreign
counterpart and agrees to respond positively to it. This may occur when a DPA
needs the help of a counterpart in terms of resources, expertise and know-how.
Countries which have recently adopted or plan to adopt legislation on privacy
and personal data protection are the main beneficiaries of this type of coopera-
tion. An illustrative example of this type of cooperation is the training session

---

1 [www.oxforddictionaries.com/definition/english/cooperation.](http://www.oxforddictionaries.com/definition/english/cooperation)
on Bindings Corporate Rules (BCR), organized by Association Francophone des Autorités de Protection des Données Personnes (AFAPDP), in July 2014, in Paris. During this meeting, experts from the French and Belgian authorities explained how to assess BCRs to representatives from Senegal, Mauritius, Tunisia, Morocco, Switzerland and Burkina Faso. Another example of this type of cooperation are the visits of representatives of the Benin authority to the French, Belgian and Quebec authorities. During those visits, the hosting DPAs thoroughly explained their procedures and process so that the Benin delegation can benefit from them and refine their expertise.

What are key success factors for cooperation?

Like in any other field, a cooperation project should meet some key factors in order to achieve its goals.

Firstly, it must be a win-win project. This means that all parts should contribute and benefit from cooperation. It is relevant to make it clear that neither the contribution nor the benefits are necessary financial.

Secondly, cooperation projects should have clear, precise and reachable objectives engaging reasonable efforts, important milestones with tangible deliverables and measurable indicators allowing managers to assess the performance and success of the project.

Thirdly, if the project cooperation involves one partner assisting the other, as in projects involving the transfer of expertise, then the beneficiary partner should be autonomous within a reasonable period and ask only for assistance in domains it can’t develop alone without disproportionate efforts and resources.

Finally, the project leader should develop appropriate mechanism that will perpetuate the results and the achievements of the project.

What are the expectations of new DPAs in terms of cooperation?

New DPAs face the challenge of setting up a new institutional structure capable of enforcing new legislation and implement a new culture in an efficient manner. To meet the challenge, they need sufficient financial resources, competent human resources, a lot of work, patience and perseverance to overcome all the problems that will definitely arise. Nevertheless, to meet the challenge and succeed in a short period of time, as they are often expected to do, they need to be assisted by their mature foreign counterparts.
At this point, it is relevant to ask at least two questions. Firstly, do all new DPAs need the same kind and form of assistance? And secondly, why would a more experienced DPA bear the additional cost of assistance, despite the lack of resources which all DPAs are facing?

The answer to the first question is obvious. DPAs in general, and new ones particularly, are subject to various constrains, as a result of which they vary as far as their “maturity” is concerned. Consequently, there are DPAs which may need financial assistance because they do not have a sufficient budget and not enough personnel to fulfill basic tasks. Another group of DPAs may need assistance to have access to the know-how of more experienced DPAs to improve processes and doctrine. This know-how can concern:

- The strategy of communication. Indeed, all new DPAs face the challenge of installing a new culture aiming to set the equilibrium between institution’s need to process personal data in their daily tasks, on one hand, and the right of data subjects in privacy protection, on the other. To obtain this equilibrium, new DPAs need other DPAs’ expertise to define the right targets, appropriate messages and relevant channels. By leveraging other DPAs experience, new DPAs can set up an efficient communication strategy to initiate a society project aiming to change mentalities and habits.
- Law enforcement, especially on how to perform in-site investigations and controls to ensure that personal data processing are in-line with the law and that data subjects rights are well respected.
- Legal and technological monitoring to face the rapid evolution of technology devices using intrusive personal data.

Still another group of DPAs will just need to coordinate with other authorities to achieve common goals, such as extending protection beyond frontiers, facing challenges triggered by global and mass processing of personal data and finally anticipating new technological, legal and societal trends that may affect privacy and personal data protection. Currently, the CNDP has a sufficient budget exceeding USD 1.5 million and ensures the accomplishment of the major tasks of DPAs, such as instruction of data controller notifications, data subject complaints processing, investigation, legal monitoring, etc. Nevertheless, it still needs to make great efforts to fill the gap between its performance and those of its European and Canadian counterparts.

Concerning the second questioning raised above, more experienced DPAs assist the new ones because national protection will always be flawed if there is not a global one. Indeed, due to transborder flow of information and globalization of processing, each DPA should rely on its counterparts to extend protection beyond national frontiers.
Ongoing cooperation programs and tools in Morocco

Since 2008, Morocco utilized the European experience in privacy and personal data protection, especially that of the French Authority (CNIL), to prepare and adopt its own legislation and to establish an independent authority – the CNDP. After its establishment, the CNDP followed the same path and relied on its counterpart’s experience and expertise to set up its institutional structure; its procedures and forms it uses to interact with other subjects involved (data subjects and data controllers).

At first hand, the CNDP relied on public information made available online by European and Canadian DPAs to learn other DPAs’ achievements, tools and doctrine. Whenever appropriate, the CNDP adapts these valuable resources to the Moroccan context before using them internally.

Thereafter, some of the CNDP’s representatives visited the French DPA (CNIL) which shared with them certain valuable materials and information concerning its institutional organization and business process.

Apart from the visits mentioned above, bilateral cooperation with European DPAs may have some good days ahead. Indeed, European authorities in charge of personal data protection were invited to submit a bid, in November 2014, in response to a call for tenders, published by the European Union. The tender in question aims to set up a light twinning program (LTP) between the CNDP and an European DPA in order to strengthen personal data protection in Morocco through the enhancement of the CNDP’s institutional structure. The projected LTP consists of the following five axis:

1. Reviewing the legal framework protecting personal data in Morocco and preparing the appropriate amendments that will fill the gap, if there is any, between Moroccan legislation and that of Europe, especially as regards the 108 Convention of the Council of Europe (CoE) and the European Union Directive 95/46.
2. Strengthening the institutional organization of the CNDP through the modernization of its business processes. This may be achieved by adapting those of the European twin DPA while taking into account the local context and the constraints of the CNDP.
3. Ensuring that the control and investigation department is operational and efficient.
4. Developing CNDP’s human resources skills and perpetuate the LTP’s gains by setting up human resources (HR) training program and preparing a manual of procedures.
5. Raising awareness of privacy and personal data concepts in Morocco by organizing seminars and preparing educational materials such as leaflets, manuals, cartoons, etc.
On the same line, the German Government, through its embassy in Rabat, has approved a cooperation project between its international agency for development and cooperation, GIZ, and the CNDP. This project, complementary to the EU’s LTP project mentioned above, will allow the Moroccan DPA to benefit from the German experience and expertise as regards privacy and personal data protection. Concrete actions will be agreed upon between the CNDP and GIZ.

Finally, the CNDP and its Belgium counterpart, the CPDP, have signed, in November 2014, an agreement which will pave the path to solid cooperation between the two authorities. The agreement will allow the signatories:

1. To jointly process notifications relating to transfer of personal data between Morocco and Belgium.
2. To mutualize their efforts in order to examine data subject complaints, involving both authorities.
3. To set up industry-specific frameworks that regulate transfers of personal data between the two countries. Corporations which use those frameworks will be allowed to transfer personal data with minimal administrative formalities.

In addition to bilateral cooperation, the CNDP joined some important international bodies that offer their members a space to exchange experiences and to discuss hot topics and common challenges on privacy and personal data protection in order to adopt common and harmonized solutions whenever appropriate.

In terms of representativeness and number of participants, the most important is the International Conference of Data Protection and Privacy Commissioners (ICDPPC), which accredited the CNDP as Data Protection Authority in its annual meeting, held in 2011 in Mexico. Since then, the CNDP took part to all ICDPPC’s annual meetings which took place in Mexico, Uruguay, Poland and Mauritius, respectively, in 2011, 2012, 2013 and 2014. The ICDPPC took many initiatives aiming to develop cooperation between DPAs. The most important are:\(^2\)

- The adoption, in 2007 in Montreal, of a resolution that encourages commissioners to further develop their efforts to support international cooperation and to work with international organizations to strengthen data protection worldwide.
- The adoption in 2011, in Mexico, of another resolution on privacy enforcement coordination at international level. This established three work streams. One was to set up an international enforcement coordination working group (IECWG) with the aim of creating specific

\(^2\) Report and website of the 36th ICDPPC.
mechanisms to put international enforcement coordination forward; the second was to hold a global annual event to discuss international enforcement coordination; while the third was to encourage all data protection/privacy authorities (DPAs/PEAs) to internally undertake some work in order to understand any legal, technical or political barriers they may have in engaging in international enforcement cooperation.

- The adoption of a resolution on digital education in the ICDPPC’s annual meeting, held in Poland in 2013, whose topic was “the application of society. What consequences do mobile apps have for society and protection and how should data protection regulators respond to the challenges?

- The 36th conference of the ICDPPC, held in Mauritius in 2014, adopted a declaration on the Internet of things and resolutions on big data, enforcement cooperation, global cross border enforcement cooperation agreement and privacy on the digital age.

Another international organization on which CNDP relies on in developing cooperation is the AFAPDP. The AFAPDP endeavors to promote the culture of privacy and data protection among French speaking countries. For this reason, it adopted, during its annual conference held in Marrakech in 2013, many resolutions aiming to enhance cooperation and coordination among its members. The most important are:

1. Resolution on the use of Binding Corporate Rules (BCR) to regulate cross-border personal data flow among members of the AFAPDP. The preparation of this resolution was assigned to a group of experts chaired by the Moroccan and Belgian DPAs.

2. Resolution on digital education promotion.

3. Resolution to encourage governments to greater transparency in processing personal data.

The last but not least, the \textit{ad hoc} committee on data protection (CAHDATA) which will submit to the Committee of Ministers proposals for the modernization of the Convention 108 and its additional protocol for the Protection of Individuals with regard to Automatic Processing of Personal Data. Morocco, which needs only to file the ratification instruments to achieve its ratification process to this convention, is contributing actively to its modernization process either by commenting on the proposals of amendments or by attending the CAHDATA meetings.
Projected cooperation

The CNDP will continue to encourage and adhere to all initiatives aiming to promote the development of the culture of privacy and enforcement of personal data legislation through cooperation and coordination among DPAs. It is in this spirit that it is considering the opportunity to join the Global Privacy Enforcement Network (GPEN) and to the International Working Group on Data Protection in Telecommunication (IWGDPT), commonly known as the Berlin Group.

Does cooperation between young DPAs make sense?

At first sight, cooperation between two young DPAs is of no relevance, as they both need assistance to become more performant. This opinion is, however, wrong, as this type of cooperation can be beneficial for both. In fact, all young DPAs face the same problems and constraints and follow the same path. First, they have to set up new institutions from scratch and lead a change-management policy to introduce “privacy and data protection” as a new concept to the society.

Because of these similarities and particularities, cooperation with a counterpart DPA with similar level of maturity may be more useful than cooperation with more experienced ones as the latter may have doctrines and practices which do not suit a society discovering “privacy and data protection”. Moreover, young DPAs can coordinate and leverage each other’s experience to solve problems characterizing new DPAs and that more experienced ones faced many decades ago.

Though the CNDP was created just few years ago, its achievements are very encouraging; also, it gained knowledge that may be shared with other DPAs or with countries planning to adopt new legislation on personal data protection.

It is for this reason that the International Organization of La Francophonie (IOF) invited the CNDP to present the Moroccan experience, relating to the enforcement of personal data protection legislation, to representatives of African countries that don’t have a specific legislation on privacy and personal data protection yet. This initiative took place in a dedicated workshop during the African Internet Governance Forum (AfIGF 2013), organized, in September 2013 in Nairobi, by the United Nations Economic Commission for Africa (UNECA), the Kenyan Government and the IOF.

Following the same logic, the Russian DPA (Roscomnadzor) invited its Moroccan counterpart to the 5th edition of the international data protection
conference held in Moscow in October 2014. At the conference, representatives of Russia, Turkey, Albania, Malta, Tajikistan, Bosnia-Herzegovina, Brazil, Kazakhstan, Vietnam, Council of Europe, Belgium and Morocco were offered the opportunity to present their respective doctrine as regards some topical issues, such as equilibrium between privacy and freedom of expression, benefits and risks of hosting personal data on the cloud, the importance of international cooperation in dealing with the cross-border flow of personal data, transnational processing of personal data, etc.

Moreover, the CNDP has also received delegations from some African countries – Mali, Burkina Faso and Senegal – with which it shares the will to strengthen collaboration in order to exchange knowledge and regulate cross-border flow of personal data.

**Conclusion**

Cooperation has an important role in reinforcing protection beyond frontiers, helping new authorities improve their processes and doctrine and creating synergy among DPAs to achieve common goals. That is why it has an important role in the CNDP’s strategy.

The CNDP will always look, when appropriate, for more experienced DPAs’ expertise to improve specific and targeted knowledge it can not develop alone.

On the other hand, it is open to contributing to the worldwide protection of personal data either by sharing its humble experience with new authorities or by helping mature authorities improve protection of the personal data imported from or exported to Morocco.
“It will be a truism to state that globalisation and recent rapid development of information and communications technologies have resulted in increased trans-border personal data transfers and – at the same time – in the elevation of corresponding risks. This phenomenon both has placed the governance of privacy and personal data protection at the international level and has made data privacy violations with cross-border implications much more frequent. As a result, there grew a critical need for stronger, more enhanced and more efficient cross-border cooperation between relevant supervisory authorities, i.e. between those public bodies that are tasked with “the day-to-day protection of data privacy”, on whose shoulders “lies the main burden of effective protection”.

The status quo of such cooperation leaves much to be desired. Nowadays – to ensure an appropriate level of protection of privacy and personal data and to investigate and prosecute violations, should they occur – these supervisory authorities face constraints by way of human and/or budgetary shortages, practical, institutional and legislative set-ups and similar factors. Often, due to the lack of cooperation and coordination, these resource-constrained authorities may also investigate the same privacy issue, which is, in effect, a duplication of effort.

For these reasons, policy-makers, authorities themselves and academics – since as early as 2000s – became preoccupied with diagnosing the problem and with the quest for solutions. […]

The PHAEDRA research project, or “Improving Practical and Helpful cooperation between Data Protection Authorities” (2013–2015), co-funded by the EU under its Fundamental Right and Citizenship Programme, has been aimed precisely to contribute to this debate. […]

This book is composed of selected interventions made at the final conference of the PHAEDRA project, held on 12 December 2014 in Kraków, Poland. These contributions are preceded by invited comments written by the experts in the field. Each of these papers – in one way or another touching upon various aspects of cooperation between supervisory authorities – contributes to the unambiguous conclusion that the efficiency of such cooperation is an essential element of the effective protection of the fundamental rights to privacy and personal data protection.”

– from Introduction
by the editors