Cooperation among data privacy supervisory authorities by analogy: lessons from parallel European mechanisms

Deliverable D2.1
version #3.5 final

Antonella Galetta
Dariusz Kloza
Paul De Hert

April 2016

The PHAEDRA II (2015-2017) project is co-funded by the European Union under the Fundamental Rights and Citizenship Programme (JUST/2013/FRAC/AG/6068).

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

Permanent link:

<table>
<thead>
<tr>
<th>Authors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Partner</td>
</tr>
<tr>
<td>Antonella Galetta</td>
<td>VUB-LSTS</td>
</tr>
<tr>
<td>Dariusz Kloza</td>
<td>VUB-LSTS</td>
</tr>
<tr>
<td>Paul De Hert</td>
<td>VUB-LSTS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contributors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Partner</td>
</tr>
<tr>
<td>Auke Willems</td>
<td>VUB-FRC</td>
</tr>
<tr>
<td>(anonymous)</td>
<td>(anonymous)</td>
</tr>
<tr>
<td>(anonymous)</td>
<td>(anonymous)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal Reviewers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Partner</td>
</tr>
<tr>
<td>Cristina Pauner</td>
<td>UJI</td>
</tr>
<tr>
<td>Rosario García Mahamut</td>
<td>UJI</td>
</tr>
<tr>
<td>Artemi Rallo</td>
<td>UJI</td>
</tr>
<tr>
<td>Beatriz Tomás</td>
<td>UJI</td>
</tr>
<tr>
<td>David Barnard-Wills</td>
<td>TRI</td>
</tr>
<tr>
<td>Dan J.B. Svantesson</td>
<td>Advisory Board</td>
</tr>
<tr>
<td>Sophie Kwasny</td>
<td>Advisory Board</td>
</tr>
<tr>
<td>Anna Zawiła</td>
<td>GIODO</td>
</tr>
<tr>
<td>Maciej Kawecki</td>
<td>GIODO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Institutional Members of the PHAEDRA II Consortium</th>
<th>Role</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vrije Universiteit Brussel (VUB)</td>
<td>Project Coordinator</td>
<td>vub.ac.be/LSTS</td>
</tr>
<tr>
<td>Research Group on Law, Science, Technology and Society (LSTS)</td>
<td>Partner</td>
<td>triilateralresearch.com</td>
</tr>
<tr>
<td>Trilateral Research Ltd. (TRI)</td>
<td>Partner</td>
<td></td>
</tr>
<tr>
<td>Biuro Generalnego Inspektora Ochrony Danych Osobowych (GIODO)</td>
<td>Partner</td>
<td>giodo.gov.pl</td>
</tr>
<tr>
<td>Universidad Jaume I (UJI)</td>
<td>Partner</td>
<td>uji.es</td>
</tr>
</tbody>
</table>
Table of Contents

EXECUTIVE SUMMARY ........................................................................................................ 5
LIST OF ABBREVIATIONS .................................................................................................... 6

1 INTRODUCTION .................................................................................................................. 7
  1.1 PURPOSE AND SCOPE OF THIS REPORT .................................................................... 7
  1.2 BACKGROUND TO THE PHAEDRA PROJECTS .......................................................... 7
  1.3 RATIONALE FOR THE COMPARATIVE ANALYSIS ..................................................... 8
  1.4 STATE OF THE ART ...................................................................................................... 9
  1.5 TERMINOLOGY ........................................................................................................... 9
  1.6 METHOD .................................................................................................................... 10
    1.6.1 Overview ................................................................................................................. 10
    1.6.2 Selection criteria for the analysis ........................................................................... 11
    1.6.3 Taxonomy of EU cooperation mechanisms ......................................................... 12
    1.6.4 Barriers and obstacles to the cooperation of supervisory authorities
         in the area of data privacy law ................................................................................. 14

2 COMPARATIVE ANALYSIS ................................................................................................ 18
  2.1 MIGRATION AND BORDER CONTROL COOPERATION ........................................... 18
    2.1.1 Legal framework .................................................................................................... 18
    2.1.2 General overview .................................................................................................. 19
      (a) Schengen Information System II ............................................................................ 19
      (b) Visa Information System ...................................................................................... 20
      (c) Eurodac .................................................................................................................. 21
      (d) EU-Lisa .................................................................................................................. 21
      (e) Customs Information System ................................................................................. 21
      (f) Protection of personal data in the mechanisms
          for immigration and border control cooperation .................................................. 22
          i) Sui generis personal data protection regime ...................................................... 22
          ii) Data subject rights ............................................................................................. 22
          iii) Cooperation ...................................................................................................... 23
          iv) Supervision ....................................................................................................... 23
    2.1.3 Observations ........................................................................................................ 24
      (a) Firm legal basis ...................................................................................................... 24
      (b) Extraterritoriality ................................................................................................... 29
      (c) Use of technology .................................................................................................. 31
      (d) Time ....................................................................................................................... 32
      (e) Multilingualism ..................................................................................................... 33
          i) General observations .......................................................................................... 33
          ii) Multilingualism in migration and border control cooperation ....................... 33
      (f) Costs ....................................................................................................................... 34
      (g) Geographical scope .............................................................................................. 36

  2.2 PRIVATE INTERNATIONAL LAW .................................................................................... 38
    2.2.1 Legal framework .................................................................................................. 38
    2.2.2 General overview .................................................................................................. 39
      (a) Rationale of private international law .................................................................... 39
      (b) Development of EU private international law ....................................................... 39
    2.2.3 Observations ........................................................................................................ 41
      (a) Mutual trust ............................................................................................................ 41
      (b) Gradual development ............................................................................................ 44
      (c) Multilingualism ..................................................................................................... 45

  2.3 CONSUMER PROTECTION COOPERATION .............................................................. 48
    2.3.1 Legal framework .................................................................................................. 48
    2.3.2 General overview .................................................................................................. 48
(a) Consumer protection cooperation (CPC) ................................................................. 48
(b) European Consumers Centres Network (ECC-Net) .................................................... 51
(c) Online dispute resolution ......................................................................................... 52
2.3.3 Observations ........................................................................................................... 55
(a) Multilingualism ......................................................................................................... 55
(b) Use of technology ..................................................................................................... 55
(c) Costs ......................................................................................................................... 59
(d) Gradual development .............................................................................................. 59
(e) Coordinated enforcement activities (‘sweeps’) ......................................................... 59
(f) Alternative Dispute Resolution (ADR) .................................................................... 61

2.4 COMPETITION LAW COOPERATION ..................................................................... 63
2.4.1 Legal framework .................................................................................................... 63
2.4.2 General overview .................................................................................................. 63
2.4.3 Observations .......................................................................................................... 65
(a) Firm legal basis ......................................................................................................... 65
(b) Use of technology ..................................................................................................... 68

2.5 CRIMINAL JUSTICE COOPERATION ................................................................. 69
2.5.1 Legal framework .................................................................................................... 69
2.5.2 General overview .................................................................................................. 70
(a) European Arrest Warrant (EAW) ............................................................................. 70
(b) European Evidence Warrant .................................................................................... 71
(c) European Investigation Order ................................................................................... 71
(d) Eurojust ........................................................................................................... 71
(e) A proposal for the European Public Prosecutor’s Office (EPPO) ............................ 73
(f) Europol ...................................................................................................................... 74
(g) Protection of personal data in criminal justice cooperation .................................... 75
(i) Eurojust ........................................................................................................... 75
(ii) Europol .................................................................................................................... 76
2.5.3 Observations .......................................................................................................... 77
(a) National differences ................................................................................................. 77
(b) Extraterritoriality ...................................................................................................... 78
(i) Conflicts of jurisdiction .......................................................................................... 78
(ii) The 2009 Framework Decision on jurisdiction in criminal proceedings ............... 79
(iii) The 2013 Directive on attacks against information systems .................................. 81
(c) Geographical scope ................................................................................................. 83
(i) Eurojust ................................................................................................................... 83
(ii) Europol .................................................................................................................... 83
(d) Multilingualism ........................................................................................................ 83
(e) Costs ......................................................................................................................... 83
(f) Use of technology ..................................................................................................... 83
(g) Time ........................................................................................................................ 84

2.6 FUNDAMENTAL RIGHTS (IN PASSIM) ..................................................................... 86
2.6.1 Legal framework ................................................................................................. 86
2.6.2 General overview ............................................................................................... 86
(a) European Union Agency for Fundamental Rights (FRA) ........................................... 86
(b) European Network of Equality Bodies (Equinet) ....................................................... 89
(c) European Information Network on Racism and Xenophobia (RAXEN) ............... 89
(d) European Network Against Racism (ENAR) ................................................................ 90
2.6.3 Observations .......................................................................................................... 90

3 MATRIX ....................................................................................................................... 91

4 CONCLUSIONS ......................................................................................................... 92

5 BIBLIOGRAPHY .......................................................................................................... 95
Executive summary

It has been well argued that cross-border cooperation among supervisory authorities in data privacy law ('cooperation'), be it in the European Union (EU) or elsewhere, is still in its infancy. There is a critical need to strengthen such cooperation to cope with challenges posed by recent technological developments and globalisation in order to offer practical, effective and efficient protection of (the right to) data privacy.

The present report looks comparatively at six areas of cross-border cooperation of relevant authorities provided for in the laws of the EU, i.e. in migration and border control, private international law, consumer protection, competition law, criminal justice and fundamental rights. It does so because some of cooperation mechanisms therein, or elements thereof, have proven to be mature, efficient and successful enough and thus could offer valuable input how to increase efficiency of cooperation in EU data privacy law.

The present report concludes with 14 lessons to be adapted to the reality and needs of cooperation within the EU and justifies the way in which these lessons could be useful to that end.
## List of abbreviations

ADR alternative dispute resolution  
APEC Asia-Pacific Economic Cooperation  
B2B business-to-business  
B2C business-to-consumer  
CFR Charter of Fundamental Rights of the European Union  
CJEU Court of Justice of the European Union  
CoE Council of Europe  
DG Directorate-General [of the European Commission]  
DG COMP Directorate-General for Competition  
DG JUST Directorate-General for Justice and Consumers  
DPA data protection authority  
EC European Community; European Commission  
ECB European Central Bank  
ECHR European Convention on Human Rights  
ECN European Competition Network  
ECtHR European Court of Human Rights  
EDPB European Data Protection Board  
EDPS European Data Protection Supervisor  
EEA European Economic Area  
EFTA European Free Trade Agreement  
EPPO European Public Prosecutor Office  
EU European Union  
FP7 7th Framework Programme for Research and Development  
GDPR General Data Protection Regulation  
GPEN Global Privacy Enforcement Network  
ICANN Internet Corporation For Assigned Names and Numbers  
ICC International Criminal Court  
ICPEN International Consumer Protection and Enforcement Network  
ICN International Competition Network  
ICT information and communications technologies  
IT information technology  
JIT joint investigation team  
MoU memorandum of understanding  
MS member state  
NCA national competition authority  
NEB national enforcement body  
NFP national focal point  
NGO non-governmental organisation  
OCC on-call coordination  
ODR on-line dispute resolution  
OLAF European Anti Fraud Office (Office européen de lutte antifraude)  
OSCE Organisation for Security and Cooperation in Europe  
PC privacy commissioner  
PIL private international law  
SLO single liaison officer  
TEC Treaty establishing European Community  
TEU Treaty on the European Union  
TFEU Treaty on the Functioning of the European Union  
UDRP Uniform Domain-Name Dispute-Resolution Policy  
UK United Kingdom of Great Britain and Northern Ireland  
UN United Nations  
USA United States of America

1 Abbreviations and acronyms used in Fig. 2 (page 12) not reproduced here.
1 Introduction

1.1 Purpose and scope of this report

By looking comparatively at parallel legal areas, this report offers possible solutions for overcoming contemporary barriers, obstacles and inefficiencies to cooperation among supervisory authorities in the area of data privacy law. More specifically, it aims at analysing which cooperation mechanisms in the laws of the European Union (EU), or elements thereof, that have already achieved relative maturity, efficiency – and thus success – and why, could be adapted to the reality and needs of cooperation in data privacy law with a view to increasing its efficiency.

However, the present analysis is not meant to be exhaustive nor objective. It is not exhaustive since the resources available within the PHAEDRA II project have limited its scope.2 (While preparing the present report, we have concluded such a comparative exercise would merit a separate research project.) It is neither objective since it rather constitutes a ‘cherry picking’ of the best elements that we would find simply useful, having earlier identified and analysed the many barriers and obstacles to the efficiency of cooperation.

Consistent with the foregoing, the main aim of this report is not to propose any optimal solution to the many problems of cross-border cooperation. (This is expected from the final report of the present project, due in January 2017.) Instead, its aim is – by informing the debate – to inspire the quest for these solutions. Therefore, we decided to work, at this stage, predominantly on ‘raw’ material. This is for the ease for policy-makers who are being offered raw legal texts to be used in their work. Extensive quotations from legal instruments as well as academic and policy writings justify our choices. Thus this report is structured predominantly as texts and materials. It has been written on the basis of the law as it stood on 1 April 2016.

The picture on the cover depicts an ideal of cooperation among supervisory authorities: two of them work side-by-side, occupied by an activity requiring a great deal of meticulousness. The photo entitled ‘Knitting Together’ is made by Kristina Alexanderson and licensed under Creative Commons.3

Editors welcome comments and suggestions at antonella.galetta@vub.ac.be, dariusz.kloza@vub.ac.be and paul.de.hert@vub.ac.be, respectively.

1.2 Background to the PHAEDRA projects

The main goal of the PHAEDRA II project – or “Improving Practical and Helpful co-operation between Data Protection Authorities II” (2015-2017) – is to identify, develop and recommend measures for improving practical cooperation between European Data Protection Authorities.4

The PHAEDRA II project represents a natural continuation of an earlier project under the same name and builds on its results. The first PHAEDRA project (2013-2015) focused on cooperation and coordination mechanisms between data protection authorities (DPAs), privacy commissioners (PCs) and privacy enforcement agencies (PEAs) (‘supervisory authorities’) around the world. It was aimed at adding value, complementing and supporting the initiatives of these supervisory authorities to improve international cooperation and coordination among them. The project analysed the state-of-the-art on the matter and – having interacted with supervisory authorities via interviews, surveys and workshops – advised policy-makers and supervisory authorities themselves how to improve their practical cooperation and coordination, in parallel raising awareness about the problem at stake.

While the first PHAEDRA project focused on their cooperation on a global scale, the core interest of the second lies in the practical cooperation of European DPAs. PHAEDRA II is focused on the challenges for cooperation arising both from the reform of the European data protection framework as well as from the EU framework in force. The project tackles three of the biggest challenges facing European DPAs: ensuring consistency, sharing different types of information (including confidential or otherwise privileged information) and coordination and cooperation regarding enforcement actions.

---

2 Cf. infra, at 1.2.
To that end, till the time of writing, the PHAEDRA II project consortium has interviewed supervisory authorities as to their views on the impact of the data protection framework reform on their cooperation in the EU (cf. Barnard-Wills and Wright 2015) and subsequently identified best practices and lessons that supervisory authorities can learn and/or adopt to improve their practical cooperation (cf. Barnard-Wills and Papakonstantinou 2016). In parallel, the project maintains a repository of leading decisions in individual cases with cross-border implications, supplemented by a collection of most significant normative documents in the field as well as a blog commenting on recent developments concerning cooperation.6

Among the remaining activities of the PHAEDRA II project, there is a comparative analysis what the notion of ‘cooperation’ of supervisory authorities in the (reformed) data privacy law in the EU can learn from their counterparts in other areas of law with a view to increase its efficiency. The present report concludes this activity. Further work will include an in-depth legal analysis of cooperation mechanisms in the adopted text of the General Data Protection Regulation (GDPR)7 (i.e. one-stop-shop, consistency mechanisms and the European Data Protection Board [EDPB]) as well as a set of final recommendations for achieving the efficiency of cooperation.

1.3 Rationale for the comparative analysis

As pointed out by many scholars (cf. e.g. Raab 2010; Raab 2011; Kloza and Mościbroda 2014; Wright and De Hert 2016) and as the first PHAEDRA project (2013-2015) confirmed (cf. e.g Kloza and Galetta 2015; De Hert, Kloza, and Makowski 2015), cross-border cooperation among supervisory authorities in data privacy law, be it in the European Union (EU) or elsewhere, is still in its infancy. Therefore it needs to be strengthened in order to:

(a) cope with contemporary challenges posed by both globalisation and information and communications technologies (ICT),
(b) offer adequate, ‘practical and effective’ protection of the fundamental rights to privacy and personal data protection (as far as the EU is concerned), and
(c) achieve efficiency, i.e. produce effects with the least waste of resources.

Methodologically speaking, debates addressing the question of improvement of such cooperation often focus on overcoming the many barriers and obstacles supervisory authorities presently face (cf. Sect. 1.6.4). And this quest for solutions habitually stays within the domain of data privacy law.

However, cross-border cooperation among relevant authorities has represented a challenge not only in data privacy law but also in many other legal areas. Looking only at the EU, some of cooperation mechanisms, or elements thereof, have proven to be mature, efficient and successful enough. These include cooperation in the areas of (1) migration and border control, (2) private international law (PIL), (3) consumer protection, (4) competition law, (5) criminal justice and (6) fundamental rights. The barriers and obstacles to cross-border cooperation among supervisory authorities, which are invoked nowadays in data privacy law, represented matters of concern to policy makers and legal practitioners already as early as in the beginning of European integration, when the premises for cross-border cooperation in many areas of EU law were laid down. To a certain extent, it is somehow surprising that very little attention thus far has been paid to the ways in which parallel cooperation mechanisms have overcome barriers and obstacles they had encountered.

---

This analysis is particularly timely as the upcoming enactment of the GDPR as well as the pending modernisation of Council of Europe’s Convention 108\(^8\) – despite both bringing significant changes to the cooperation within the scope of their application – on the one hand, raise a number of controversies, and on the other, leave a fistful of practical issues open.


[…]. One might argue that the arrival of the General Data Protection Regulation (GDPR) – the text of which has been agreed in December 2015 but not yet passed into law – would render our exercise belated. We argue quite on the contrary. While the GDPR would bring some significant yet sometimes controversial improvements – such as the mere obligation to cooperate, one-stop-shop and mechanisms for consistent decision making – it would also leave a number of open questions, pertaining predominantly to the practical aspects of cooperation, to be answered during the *vacatio legis*. Both these controversies and issues left open make our comparative exercise still timely. […]

1.4 State of the art

The comparative analysis exercise has been already performed partially within the framework of the first PHAEDRA project (2013-2015), namely:

(a) general overview of possible cooperation mechanisms for comparative analysis (cf. De Hert and Boulet 2014, 19–33);

(b) competition law
  – the functioning of the International- (ICN) and European Competition Network (ECN) and how these could be adapted to the needs and reality of data privacy law (cf. Kloza, Mościbroda, and Boulet 2013; Kloza and Mościbroda 2014);

(c) criminal law:
  – the trouble with overlapping jurisdictions and requests for mutual legal assistance (De Hert and Willems 2015, 49–76),
  – the possible use of criminal sanctions for the enforcement of data privacy law (De Hert 2014, 262–268; De Hert and Boulet 2016);

(d) public international law:
  – global governance of data privacy (De Hert and Papakonstantinou 2013, 272–324).

Further literature could include:

  – setting standards for cooperation (Raab 2010, 291–302), (Raab 2011, 195–213), (Gaisbauer 2013, 185–201);
  – areas of cooperation of DPAs (Jori 2015, 133–143);
  – an analysis of supervisory authorities’ prospects to influence the international data privacy agenda and cooperation (Zalnieriute 2016, 31–54).

1.5 Terminology

_Dariusz Kloza and Antonella Galetta, Towards efficient cooperation between supervisory authorities in the area of data privacy law, Brussels Privacy Hub (2015)\(^9\)_

[…]. 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

---

\(^8\) Although the analysis of the Council of Europe (CoE) modernised Convention for the Protection of individuals with regard to automatic processing of personal data (hereinafter: modernised Convention 108; cf. CAHDATA(2014)RAP03Abr) lies outside the scope of the present report, the editors are of the opinion that both pending reforms of data privacy law on the European continent – i.e. EU and CoE – should be regarded as interconnected.

\(^9\) Original footnotes omitted. Emphasis ours.
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 term “data privacy” – embracing in particular the European understanding of “personal data protection” and the Anglo-Saxon one of “informational privacy” – in order to “avoid terminology that might seem focused too much on a particular legal system” (Kuner et al. 2014).

Third, for similar reasons, we have selected the term “supervisory authority” 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). Only some of these bodies are independent regulatory authorities, while others may be public bodies tasked prima facie with other issues, but dealing with data privacy too. We opt for this all-encompassing approach as independence is not always a requirement for cooperation in data privacy law and such cooperation may involve authorities at various levels. Still, we are aware that supervisory authorities are not endowed with the same functions and powers (Bennett and Raab 2006) as well as resources, which is often reflected in their willingness and ability to cooperate as well as in the scope thereof. (We are also aware that not only public bodies might be involved in the protection of data privacy, e.g. NGOs, but these do not focus on enforcement and thus fall outside the term “supervisory authorities”.)

Fourth, by a “cross-jurisdictional data privacy violation” we refer to a breach of data privacy laws producing effects or implications in more than one jurisdiction.

Finally, by “cooperation” we mean a spectre of activities undertaken together by supervisory authorities in fulfilling their functions and duties. This cooperation is not of a uniform nature and can range from “soft” forms, such as policy shaping, exchange of good practice, training, study visits, research or education, to “hard” ones, like enforcement of data privacy laws in cross-jurisdictional cases. […]

Furthermore, by ‘cooperation mechanisms’ we understand a totality of arrangements put up in place to establish cooperation – be it legal frameworks (substantive and procedural law), actors (institutions, bodies, agencies, independent regulatory agencies, etc.) and policies.

### 1.6 Method

#### 1.6.1 Overview

The present report applies a comparative legal analysis of relevant secondary laws of the EU, i.e. international agreements that the EU and/or its Member States are bound by, directives, regulations and decisions. This is occasionally supplemented by an analysis of academic literature, policy documents and media coverage.

The report first attempts to identify and categorize as many existing cooperation mechanisms in the EU law as possible. Subsequently, it selects six of them for further analysis, using the criteria developed in Sect. 1.6.2. Next, it turns to an analysis of each of them (Sect. 2.1-2.6), offering their legal bases in the EU secondary law, a general overview of their functioning and a ‘cherry picking’ of these elements and practices that might be useful for overcoming barriers, obstacles and inefficiencies of contemporary cooperation mechanisms in data privacy law. [These have been identified earlier in (Barnard-Wills and Wright 2014; Barnard-Wills and Wright 2015) (Sect. 1.6.4)].

Eventually, the present report proposes 14 lessons – best elements and best practices – to be adapted to the reality and needs of the EU data privacy law and justifies the way in which these could be useful therein (Sect. 4), preceded by a ‘matrix’ of these lessons and their origins (Sect. 3). A bibliography supplements this report (Sect. 5). Fig. 1 explains the research method used.

---

10 For the ease of the reader, the legal instruments mentioned at the beginning of each section are given short names, printed in square brackets and in bold, unless the legislator has already attributed these. Extensive citations come from the legal instrument under discussion, unless stated otherwise.
1.6.2 Selection criteria for the analysis

In the first step, the existing cooperation mechanisms in the EU law have been identified and categorised using the following selection criteria:

(a) Their functioning is predominantly based on *information processing (including its sharing)* in one or another way, comprising the processing of personal data as well as confidential or otherwise privileged information (e.g. state or trade secrets);

(b) for the purposes of *giving effect to relevant laws*, be it *ex post* enforcement or *ex ante* preventive measures;

(c) in *cross-jurisdictional* situations, i.e. originating from and/or producing effects or implications in more than one jurisdiction;

(d) in *the EU*, i.e. among Members States and/or EU institutions.

The list rendered, despite its non-exhaustiveness, has proven rather to be complex (Fig. 2). In the subsequent step, due to limited resources available within the PHAEDRA II project, these results have been refined. Having applied the following criteria:

(a) *data-dependence*, i.e. the importance of processing and sharing information for giving effect to the relevant laws;

(b) *relevance* for cooperation in the area of data privacy, i.e. having achieved sufficient maturity, efficiency – and thus success, the ability to inform the debate and efforts to increase efficiency of parallel cooperation in data privacy law; and

(c) relative *maturity*, *efficiency* and *success*;

the second step has produced six cooperation mechanisms for a further analysis:

(a) migration and border control,
(b) private international law (PIL),
(c) consumer protection,
(d) competition law,
(e) criminal justice, and
(f) fundamental rights.
### 1.6.3 Taxonomy of EU cooperation mechanisms

#### Migration & border control
- **Frameworks**
  - Schengen
    - SIS II
    - VIS
  - Dublin
    - Eurodac
  - Customs Convention
    - CIS
    - FIDE
- **Supervisors (specific)**
  - SCG
  - JSA
- **Supervisors (generic)**
  - EDPS WP29
    - [EDPB]
  - EU-LISA
    - Frontex
  - SIRENE

#### Internal market
- **Competition**
  - Networks
  - ECN
- **Taxation**
  - Frameworks
    - DAC
    - EU-CH agreement
  - Advisory group
    - AEFI
- **Consumers**
  - Frameworks
    - ADR
    - ODR
  - Agencies
    - CPC
    - ECC-Net
  - Case handling
    - CPCS

#### Financial markets
- **Supervisors (generic)**
  - ESMA
  - EBA
  - EIOPA

#### Criminal law
- **Frameworks**
  - EAW
    - EEW
    - EIA
  - Bodies
    - CEPOL
    - [EPPO]
    - Europol
    - Eurojust
- **Supervisors**
  - Networks
    - JSB [EDPS]
    - JSB
  - EJTN
  - Networks
    - EJN-civil

#### Civil law
- **Frameworks**
  - Brussels I
  - Rome II
  - EEO
  - EOP
  - ESCP
  - EAPO

#### Fundamental Rights
- **Supervisors**
  - Networks
    - ENAR
    - RAXEN
    - Equinet

---

*Figure 2: Taxonomy of EU mechanisms for (enforcement) cooperation*
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Explanation</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Migration and border control</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIS II</td>
<td>Schengen Information System II</td>
<td></td>
</tr>
<tr>
<td>VIS</td>
<td>Visa Information System</td>
<td></td>
</tr>
<tr>
<td>Eurodac</td>
<td>European Dactyloscopy</td>
<td></td>
</tr>
<tr>
<td>CIS</td>
<td>Customs Information System</td>
<td></td>
</tr>
<tr>
<td>FIDE</td>
<td>Customs Files Identification Database</td>
<td></td>
</tr>
<tr>
<td>Prüm</td>
<td>Convention [...] on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration</td>
<td></td>
</tr>
<tr>
<td>EU PNR</td>
<td>EU Passenger Name Record</td>
<td>eulisa.europa.eu</td>
</tr>
<tr>
<td>EU-LISA</td>
<td>European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice</td>
<td>frontex.europa.eu</td>
</tr>
<tr>
<td>Frontex</td>
<td>European Agency for the Management of Operational Cooperation at the External Borders</td>
<td></td>
</tr>
<tr>
<td>SIRENE</td>
<td>Supplementary Information Request at the National Entries</td>
<td></td>
</tr>
<tr>
<td>SCG</td>
<td>Supervision Cooperation Group</td>
<td></td>
</tr>
<tr>
<td>JSA</td>
<td>Joint Supervisory Authority</td>
<td>wpx.cp.2019.11.30.293341</td>
</tr>
<tr>
<td>EPDS</td>
<td>European Data Protection Supervisor</td>
<td>edps.europa.eu</td>
</tr>
<tr>
<td>WP29</td>
<td>Art 29 Working Party</td>
<td></td>
</tr>
<tr>
<td>EDPB</td>
<td>European Data Protection Board</td>
<td></td>
</tr>
<tr>
<td><strong>Administrative law</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMI</td>
<td>Internal Market Information System</td>
<td></td>
</tr>
<tr>
<td>SOLVIT</td>
<td>(own name)</td>
<td>ec.europa.eu/solvit</td>
</tr>
<tr>
<td><strong>Internal market</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECN</td>
<td>European Competition Network</td>
<td></td>
</tr>
<tr>
<td>ADR</td>
<td>Alternative Dispute Resolution</td>
<td></td>
</tr>
<tr>
<td>ODR</td>
<td>On-line Dispute Resolution</td>
<td></td>
</tr>
<tr>
<td>CPC</td>
<td>Consumer Protection Cooperation</td>
<td></td>
</tr>
<tr>
<td>CPCS</td>
<td>Consumer Protection Cooperation System</td>
<td></td>
</tr>
<tr>
<td>ECC-Net</td>
<td>European Consumers Centres Network</td>
<td>ec.europa.eu/consumers/ecc</td>
</tr>
<tr>
<td>DAC2</td>
<td>Directive on Administrative Cooperation in Taxation</td>
<td></td>
</tr>
<tr>
<td><strong>EU-CH agreement</strong></td>
<td>Agreement between the European Community and the Swiss Confederation providing for measures equivalent to those laid down in Council Directive 2003/48/EC on taxation of savings income in the form of interest payments</td>
<td></td>
</tr>
<tr>
<td>AEFI</td>
<td>Automatic Exchange of Financial Account Information</td>
<td></td>
</tr>
<tr>
<td>ESMA</td>
<td>European Securities and Markets Authority</td>
<td>esma.europa.eu</td>
</tr>
<tr>
<td>EBA</td>
<td>European Banking Authority</td>
<td>eba.europa.eu</td>
</tr>
<tr>
<td>EIOPA</td>
<td>European Insurance and Occupational Pensions Authority</td>
<td>eiopeuropa.eu</td>
</tr>
<tr>
<td><strong>Criminal law</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAW</td>
<td>European Arrest Warrant</td>
<td></td>
</tr>
<tr>
<td>EEW</td>
<td>European Evidence Warrant</td>
<td></td>
</tr>
<tr>
<td>EIO</td>
<td>European Investigation Order</td>
<td></td>
</tr>
<tr>
<td>CEPOL</td>
<td>European Police College</td>
<td>epol.europa.eu</td>
</tr>
<tr>
<td>Collège européen de police</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EPPO</td>
<td>European Public Prosecutor Office</td>
<td></td>
</tr>
<tr>
<td>Europol</td>
<td>European Police Office</td>
<td>europol.europa.eu</td>
</tr>
<tr>
<td>Eurojust</td>
<td>(own name)</td>
<td>eurojust.europa.eu</td>
</tr>
<tr>
<td>JSB</td>
<td>Joint Supervisory Body</td>
<td></td>
</tr>
<tr>
<td>ECRIS</td>
<td>European Criminal Records Information System</td>
<td></td>
</tr>
<tr>
<td>ECMS</td>
<td>Europol Case Management System</td>
<td></td>
</tr>
<tr>
<td>EIS</td>
<td>Eurojust Information System</td>
<td></td>
</tr>
<tr>
<td>EJN</td>
<td>European Judicial Network</td>
<td>ejn-crimjust.europa.eu</td>
</tr>
<tr>
<td>Genocide</td>
<td>European Network for investigation and prosecution of genocide, crimes against humanity and war crimes</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JITs Network</td>
<td>Network of National Experts on Joint Investigation Teams</td>
<td></td>
</tr>
</tbody>
</table>
1.6.4 Barriers and obstacles to the cooperation of supervisory authorities in the area of data privacy law

The cooperation process nowadays faces numerous barriers, both of legal (e.g. capacity to engage in international cooperation, procedures, sharing information) and practical nature (e.g. resources, technical tools, languages, sharing costs), thus rendering it ineffective at best and at worst impossible (Kloza and Galetta 2015).

David Barnard-Wills and David Wright, “Co-ordination and co-operation between Data Protection Authorities”, Deliverable D1 of the PHAEDRA Project (2014)

Key challenges for co-operation and co-ordination remain

Situational awareness of the international privacy enforcement context is a key barrier to effective co-operation. DPAs identified a lack of information from their peers about co-operation and co-ordination activities. This highlights the important role that centralised groups with regular channels of communication can play. From the survey and interviews, legal barriers to sharing of information between DPAs appear to be less significant than may have been believed, although they remain particularly significant for some DPAs due to their legal constitution. In the absence of harmonised legislation (which may be facilitated by the GDPR) it becomes important for co-operating DPAs to understand the limitations, powers and capacities of their peers.

Limited resources that can be devoted to international working are a key issue that limits co-operation and co-ordination, whilst in part driving the desire for increasing these. DPAs have variable funding, capacity, experience and different powers in enforcement, investigation and audit, whilst some can only investigate following complaints. Responses to the survey showed that DPAs, both within Europe and externally had highly variable numbers of staff. However, converging the powers of DPAs was not seen as the highest priority for increasing co-ordination and co-operation. The WhatsApp case study suggests that co-operation on privacy enforcement is possible even across different legal regimes and with different enforcement powers.

DPAs are not the only organisations that need to be involved in co-ordination of privacy enforcement activity. Well supported DPAs and networks are better able to leverage co-operation. When they are not well supported […] then co-ordination efforts can be undermined. Similarly, whilst it is important to have closed sessions, and networks with membership limited to accredited DPAs for sensitive discussions and building common positions, it is also important to have networks that can include other authorities with some form of privacy enforcement brief, and even representatives from government, NGOs, academia and the private sector. The mix of overlapping networks currently contributes to this capacity.
Most DPAs anticipated a significant, strong impact from the passing of the GDPR in general, and particularly for co-operation between European DPAs. The stance of many DPAs towards the GDPR was optimistic, although this was often balanced with some caution, or a recognition of additional work that needed (and needs) to be done, and pending issues that would need to be resolved. In general, DPAs believed that increased co-operation under the GDPR would bring an increased administrative burden and may raise resource and capacity issues. All DPAs interviewed recognised the need for increased collaboration within the EU (which was seen by some as critical, given that a spirit or attitude of co-operation may be as important as specific legal provisions for co-operation). Several DPAs informed us that they anticipated the GDPR reforms to act as driver for more frequent co-operation. This differs from our assumption under PHAEDRA II that resource issues and the desire to avoid duplication of effort in enforcement would be primary drivers for co-operation and co-ordination.

The GDPR reform process is still ongoing. The first Trialogue sessions have commenced at the time of writing. There are ongoing discussions on consistency mechanism, one-stop shop and the legal identity, powers and role of the EDPS. There are still things to be decided, and there are still things to be worked out in practice. A still pending issue worthy of further attention is how practical co-operation required by the GDPR, particularly through the consistency mechanism, one-stop-shop and the EDPB will be resolved in practice. For example, what will become normal practice for concerned DPAs involved in investigations? What time limits will be considered acceptable in investigations? It may be the case that these norms emerge amongst the community of European DPAs over time, through their experience in this type of cooperative activity. The extent to which the GDPR will harmonise data protection in the EU is still debated. Some DPAs interviewed expressed opinions that the Regulation’s provisions would mean European DPAs had equivalent powers and roles, reducing the diversity of national implementations of data protection law, in effect creating a single regime of data protection. Others instead expressed the belief that there would still remain differences in national practice and particularly in both culture and strategy, as well as differences in size, resources, experience and economic context in which they were required to operate as a regulator. A requirement emerging from this may be the need to better understand where there will be remaining differences in areas not covered (and therefore not harmonised) by the GDPR.

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

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

Language differences remains a key topic of discussion in these interviews. **Problems raised by language** emerged in the interviews in relation to the exchange of information, communication systems, requests for assistance, repositories of decisions, public communication, and dealing with the one-stop-shop. Whilst DPAs generally felt able to communicate with their peers, either with English as a lingua franca or a set of commonly used and known European languages, communication with and from the public in different countries posed a greater challenge, as did the translation of decisions and legal documents in investigations and court cases. Translation imposes resource questions and there was uncertainty about the source of the required resources, and who should carry the cost. Working in common or shared languages, and making a decision about which to focus upon is a highly political issue. Some DPAs looked to the Commission for support in this area.

---

11 Emphasis in original.
Commission has experience in working across 24 official EU languages and has one of the largest translation services in the world.\textsuperscript{12} Further research might understand the real extent of this problem in practice, and the number of languages required for effective co-operation.

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

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

Consistent with foregoing, as well as our previous research, a number of barriers and obstacles could be identified – predominantly of \textit{practical} nature – that cooperation currently faces. These include:

1) \textbf{legality}, i.e. grounding cooperation on a binding, firm legal basis and providing a comprehensive framework therefor;

2) \textbf{national differences (legal pluralism)}, i.e. acknowledging differences among legal cultures in different jurisdictions;

3) \textbf{extraterritoriality}, i.e. both the ability and the possibility to deal with a data privacy issue (\textit{sensu largo}), to a reasonable extent, beyond the limits of their own jurisdiction, both territorial and personal;

4) \textbf{geographical broadness}, i.e. both the ability and the possibility to cooperate with a wide array of counterpart authorities and/or their organisations, to a reasonable extent;

5) \textbf{multilingualism}, i.e. the ability to deal with linguistic differences in an efficient way while, in parallel, not limiting the access to remedies (or – broader – to justice);

6) \textbf{costs sharing}, i.e. the ability to share (or otherwise mutualise) the costs of cooperation in a justified manner;

7) \textbf{use of technology}, i.e. both the ability and the possibility to increase the efficiency of cooperation by using technological means, predominantly to exchange relevant information in a safe and secure manner;

8) \textbf{time-frames}, i.e. both the ability and the possibility to deal with a data privacy issue (\textit{sensu largo}) in a timely and fast manner;

Having investigated these, we have discovered further a number of useful solutions present in the legal areas of our concerns and these include:

1) \textbf{mutual trust}, i.e. the necessity to firmly believe in the reliability, truth and ability of counterpart authorities and their officials as well as in both legal and political systems of their home jurisdictions;

2) \textbf{gradual development}, i.e. a function of the experimental nature of the issue under regulation that require careful development thereof;

3) \textbf{coordinated enforcement (‘sweeps’)}, i.e. both the ability and the possibility for the supervisory authorities to jointly investigate a data privacy issue (\textit{sensu largo} \textit{ex ante}, i.e. before a data privacy issue (\textit{sensu largo}) arises;

4) \textbf{alternative dispute resolution mechanisms (ADR)}, i.e. the use thereof for low-value disputes between data subject and data controller/processor;

5) **co-existence of formal and informal mechanisms**, i.e. the combination of mechanisms as deemed necessary for dealing with a data privacy issue (*sensu largo*).

These combined will guide our further analysis, they will serve as a main key in analysing parallel cooperation mechanisms.
2 Comparative analysis

2.1 Migration and border control cooperation

2.1.1 Legal framework

(a) Schengen Information System II [SIS II]
- 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, 19 June 1990 [CISA]13

(b) Visa Information System [VIS]

(c) Dublin System and Eurodac

Historical
- Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities (15 June 1990) [Dublin Convention]21
- Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national [Dublin II Regulation]23

In force
- Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member

---

18 OJ L 205, 07.08.2007, pp. 63–84.
State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes [...]

- Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person [Dublin III Regulation]

(d) Customs Information System [CIS]

- Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters [CIS Regulation]
- Council Regulation (EC) No 807/2003 of 14 April 2003 adapting to Decision 1999/468/EC the provisions relating to committees which assist the Commission in the exercise of its implementing powers laid down in Council instruments adopted in accordance with the consultation procedure (unanimity)
- Regulation (EC) No 766/2008 of the European Parliament and of the Council of 9 July 2008 amending Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters

(e) Prüm

- Convention of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration [Prüm Treaty]
- Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [Prüm Decision]
- Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

(f) Actors


2.1.2 General overview

(a) Schengen Information System II

The Schengen Information System II (SIS II) database represents perhaps the most important and widest EU database used for two main purposes: (1) migration and external border control as well as (2) law enforcement purposes. On the one hand, the purpose of SIS II is to ensure internal security in the Schengen states, given the absence of internal border checks. On the other, its objective is to keep non-EU citizens and unwanted aliens out of the Schengen area.
The SIS database processes information about:

(a) persons wanted for extradition to another Schengen state;
(b) a list of non-EU citizens (‘aliens’ or ‘third-country nationals’) who should in principle be denied entry to any of the Schengen states;
(c) missing persons or persons temporarily placed under police protection;
(d) persons wanted as witnesses, or for the purposes of prosecution of criminal offences or the enforcement of sentences;
(e) persons or vehicles placed under surveillance or subjected to specific checks; and
(f) objects sought for the purpose of seizure or use as evidence in criminal proceedings.

The SIS is considered a highly efficient large-scale information system enabling competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. A SIS alert not only contains information about a particular person or object but also clear instructions on what to do when the person or object has been found. The SIS further enables border guards and visa issuing and migration authorities to enter and consult alerts on third-country nationals for the purpose of refusing their entry into or stay in the Schengen states. Vehicle registration services may consult the SIS in order to check the legal status of the vehicles presented to them for registration. These authorities only have access to this single category of SIS alerts.

Since April 2013, SIS II, a more advanced version of SIS, has been put in operation. It has enhanced functionalities, such as the possibility to use biometrics, new types of alerts, the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system. SIS II also contains copies of European Arrest Warrants (EAW), which are recognised as having the same legal value as the originals, making it easier and quicker for the competent authorities to ensure the necessary follow-up [cf. Sect. 2.5.2(a)].

The SIS is in operation in all EU Member States and Associated Countries that are part of the Schengen Area. The Schengen Area, as of March 2016, encompasses most EU Member States, except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. The 22 EU Member States that are part of the Schengen Area fully operate the SIS, as do the four Associated Countries that are part of the Schengen Area (Switzerland, Norway, Liechtenstein and Iceland). Bulgaria and Romania currently only operate the SIS for the purpose of law enforcement cooperation. They will start using the SIS for the purpose of external border control as soon as the decision for lifting the internal border checks has entered into effect. Similarly, the United Kingdom only operates the SIS within the context of law enforcement cooperation. Ireland is carrying out preparatory activities to integrate into the SIS for the purpose of law enforcement cooperation. Cyprus and Croatia are enjoying a temporary derogation from joining the Schengen Area. They are currently carrying out preparatory activities to integrate into the SIS.

(b) Visa Information System

The Visa Information System (VIS) database is meant to improve the implementation of “the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data”. In particular, by exchanging visa application information among Schengen states, VIS aims to:

(a) facilitate the visa application procedure;
(b) prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application;
(c) facilitate the fight against fraud;
(d) facilitate checks at external border crossing points and within the territory of the Member States;
(e) allow identification of individuals who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States;
(f) contribute to determine the Member State responsible for examining an asylum application;
(g) contribute to the prevention of threats to the internal security of Member States.

VIS contains biometric identifiers of the applicant for a visa as well as details on the request for a visa, in particular:

(a) alphanumeric data on the applicant and on the visa requested, issued, refused, annulled, revoked or extended;
(b) a digital photograph of the applicant;
(c) 10 fingerprints of the applicant taken flat and collected digitally;
(d) links to previous applications made by the applicant which are already registered in the system (if any), as well as links to the application files of the spouse, children or other individuals travelling with the applicant.
Children under the age of 12 and persons “for whom fingerprinting is physically impossible” are exempted from the obligation to give fingerprints. This obligation does not apply to heads of states or governments and to sovereigns and members of their families.

The bodies having access to VIS are: visa issuing and police authorities from EU Member States as well as Europol. Transfer of data to third countries or international organizations may take place only in an exceptional case of urgency, with the consent of the Member State that entered the data.

(c) Eurodac

Eurodac (or ‘European Dactyloscopy’) is an asylum fingerprint database for identifying asylum seekers and irregular border-crossers that cross the external EU borders. The main purpose is to implement the Dublin Regulation by preventing ‘asylum shopping’.

The purpose of the so-called Dublin System (from the 1990 Dublin Convention, subsequently replaced by Dublin II [2003] and Dublin III [2013] regulations) is, *inter alia*, to determine which Member State is responsible for examining an asylum application by a third-country national or a stateless person. The Member State in which the asylum seeker first applies for asylum is responsible for either accepting or rejecting asylum, and the seeker may not restart the process in another Member State.

However, the Dublin System created a need to verify if an applicant has not applied already in another EU Member State. This requires to exchange information on all application lodged on a real-time basis. Furthermore, as the asylum seekers usually do not have proper documentation, it was decided that the help of biometric features – that is fingerprints – would establish their identity.

Therefore, a fingerprint database was established. Each Member State shall “promptly take the fingerprints of all fingers” of

(a) every applicant for asylum of at least 14 years of age, and
(b) every alien of at least 14 years of age who is apprehended by the competent control authorities of a Member State in connection with the irregular crossing by land, sea or air of that Member State.

Until the entry into force of Dublin III Regulation (20 July 2015), the Eurodac database could only be used for asylum purposes. The new Regulation now allows national police forces and Europol to compare fingerprints linked to criminal investigations with those contained in Eurodac for the purpose of the prevention, detection and investigation of serious crimes and terrorism.

(d) EU-Lisa

The daily management of the three above-mentioned databases is ‘outsourced’ to EU-Lisa, i.e. the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. Operational management consists of “all the tasks necessary to keep large-scale IT systems functioning in accordance with the specific provisions applicable to each of them, including responsibility for the communication infrastructure used by them”. Accordingly, EU-Lisa ensures:

- the effective, secure and continuous operation of SIS II, VIS and Eurodac;
- their efficient and financially accountable management;
- the high quality and continuity of services for users of these IT systems;
- a high level of data protection and physical security;
- an adequate project management structure for the efficient development of SIS II, VIS and Eurodac.

The Agency further ensures the functioning and operation of the communication infrastructure between the Central System and Member States, as well as the security and coordination of relations between Member States and the provider. Moreover, EU-Lisa is responsible for the training of national authorities on the technical use of SIS II, VIS and Eurodac.

(e) Customs Information System

The Customs Information System (CIS) is a computer network established to prevent, investigate and prosecute violations of customs and agricultural legislation in the EU. Data entered into the CIS relate to goods, means of transport, businesses, persons, trends in fraud, availability of expertise, goods detained, seized and confiscated and cash detained, seized and confiscated. Specific cooperation arrangements are in place under CIS between Member States as well as between them and the European Commission in order to counter the violations of European laws on customs and agricultural matters.
Protection of personal data in the mechanisms for immigration and border control cooperation

i) Sui generis personal data protection regime

Due to the specific nature of immigration and border control cooperation, short of CIS, the system of protection of personal data falls under a separate sui generis regime. It adheres to generally agreed data protection principles – e.g. data minimisation, remedies, etc. – but neither follows the general 1995 Data Protection Directive\(^\text{33}\) regime nor the one of the 2008 Framework Decision.\(^\text{34}\) Instead, each cooperation mechanism, from SIS II to Eurodac, establishes its own personal data protection rules. The level of protection, however, is significantly limited (Boehm 2011), reflecting its specific nature. In particular, the limited level of protection is to ensure the smooth functioning of migration and border control cooperation.

ii) Data subject rights

Generally speaking, one of the constitutive elements of any data privacy legal framework is the access to remedies available to an individual concerned. If we look at a data subject, in case of a violation, she can normally seek relief by complaining to the data controller, to a supervisory authority or to a court, national or – in a few situations – supranational one. Galetta and De Hert have conceptualised this access to remedies as having a three-layered approach (2015, 123–149). But “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” (Kloza and Galetta 2015, 10).

However, in certain areas, and this includes migration and border control, the scope of these access rights might be limited due to the nature and goals pursued by such control. Hence, the key element of this sui generis personal data protection framework is the data subject’s right of access.\(^\text{35}\)

Antonella Galetta and Paul De Hert, “The proceduralisation of data protection remedies under EU data protection law: towards a more effective and data subject-oriented remedial system?”, 8 Review of European Administrative Law 1 (2015)\(^\text{36}\)

[...] data protection remedies can be exercised in different ways under EU law. Three main possibilities are envisaged, as follows:

1) Data protection remedies sought before the data controller (or processor): access rights (layer 1);
2) Data protection remedies sought before DPAs (layer 2);
3) Data protection remedies sought before national courts (layer 3).

[...] Special remedial norms and procedures in the police and criminal justice area are set forth within the Schengen legal framework. Elaborated in the Convention implementing the Schengen Agreement (CISA), which established the Schengen Information System (SIS), these rules have been transposed in the so-called second-generation SIS, or SIS II. Article 58 of the Council Decision 2007/533/JHA (SIS II Decision) grants data subjects the right of access to data entered in SIS II (layer 1). Access requests can be introduced to any of the contracting parties following provisions on access to police and judicial data established at national level. If national law so provides, the national DPA decides whether information is to be communicated and by what procedures (layer 2). However, access may only be refused if ‘this is indispensable for the performance of a lawful task in connection with an alert or for the protection of the rights and freedoms of third parties’ (Article 58(4) SIS II Decision). It is stipulated that the required information should be provided ‘as soon as possible and in any event not later than 60 days from the date on which he applies for access or sooner if national law so provides’ (Article 58(6) SIS II Decision). The data subject can bring an action against national courts to obtain...


\(^{36}\) Original footnotes omitted.
access or compensation in connection with an alert relating to him (Article 59(1) SIS II Decision) (layer 3). Enhanced forms of cooperation are part of the Schengen architecture. Where a national court or authority finds a SIS report unlawful and orders the withdrawal of an alert, all contracting parties are obliged to mutually enforce this decision (Article 59(2) SIS II Decision).

Although the Schengen information system concerns data in the police and criminal justice area, we observe that it provides a satisfactory protection of data subjects’ rights. The remedial system in place therein is solid and functions well mainly because the data processing system is well structured and organised (1); the remedial system is effective (as it entails binding decisions for all contracting parties) (2) and; it establishes good cooperation mechanisms between the police, judicial and administrative authorities (3).

For example, in case of Eurodac, an asylum seeker or illegal immigrant should be informed by the Member State of the right of access to and the right to rectify the data concerning her. In particular, the data subject has the right “to obtain communication of the data relating to him or her recorded in the Central System and of the Member State which transmitted them to the Central System”. Likewise, the data subject has the right to have information corrected and erased “without excessive delay by the Member State which transmitted the data”.

In case of CIS, this database is considered as a personal data-processing system subject to the provisions of the 1995 Data Protection Directive and Regulation 45/2001.37 Persons whose personal data are processed by the CIS have the right to access, correct and delete them in accordance with the laws, regulations and procedures established by the Member State in which such rights are invoked, as well as with European data protection law. Nonetheless, a Member State may refuse access if communication would be “likely to prejudice the prevention, investigation and prosecution of operations which are in breach of customs or agricultural legislation”. Also, access may be refused when this is necessary to safeguard national security, defence, public safety and the rights and freedoms of others.

iii) Cooperation

It is worth noting that specific cooperation mechanisms exist in order to allow for the data subject to exercise her access rights. In case of VIS, specific norms on cooperation among Member States apply in the case in which a request for access, correction or deletion is addressed to a Member State other than the Member State responsible for processing the application. In this circumstance the former State has to contact the latter within a period of 14 days. A Member State can possibly refuse to correct or delete data of the applicant. However, if this circumstance occurs an explanation for the refusal should be provided and the Member State concerned should also inform the applicant on how to bring an action or complaint to the national DPA or courts.

iv) Supervision

Initially, it was the Joint Supervisory Authority (JSA) the supervised the processing of personal data in SIS. The JSA had the task of checking that the provisions of CISA were properly implemented; of examining any difficulties of application or interpretation during the operation of the SIS; of studying any problems related to the exercise of independent supervision by the national supervisory authorities of the Contracting Parties or in the exercise of access rights; and of drawing up “harmonised proposals for joint solutions to existing problems”. In more concrete terms, the JSA delivered opinions in the event that two Contracting Parties could not reach an agreement with regard to data contained in an alert that had been entered incorrectly or unlawfully; drafted harmonised proposals aimed at resolving existing problems; delivered opinions at the request of the Contracting Parties in relation to the automated processing of personal data or in relation to the entry of data in a non-automated database. The JSA consisted of representatives of the national supervisory authorities. Each Contracting Party could exercise one vote within the JSA.

The Schengen JSA ceased its activities on 9 April 2013 as a consequence of changes introduced in the shift from SIS to SIS II. Presently the protection of personal data in the framework of SIS II is ensured by the Schengen Supervision Coordination Group (SIS II SCG), consisting of national DPAs and the EDPS. As stressed by the JSA in its penultimate activity report, the new coordinated supervision under SIS II does

not lessen the level of supervision laid down by the CISA. Instead, it marks the shift from a joint supervisory regime to a coordinated system. The JSA oversaw the Schengen states whether the processing of data in the SIS was lawful. Under this new legal framework, the protection of personal data is shared between national DPAs and the EDPS, each acting within the scope of their respective competences. Hence, they have taken over the tasks and responsibilities of the JSA jointly. The new framework tasks national DPAs and the EDPS to:

- exchange relevant information;
- assist each other in carrying out audits and inspections;
- examine difficulties of interpretation or application of the Council Decision;
- study problems with the exercise of independent supervision or in the exercise of subjects’ rights;
- draw up harmonised proposals for joint solutions to any problems; and
- promote awareness of data protection rights.

To this end, national DPAs and the EDPS meet twice a year and issue a joint report on activities every two years which is transmitted to the European Parliament, the Council, the European Commission and the Management Authority. The first meeting of the SIS II SCG was held on 11 June 2013.

The shift from the joint supervisory regime of SIS to the coordinated system of SIS II implies that national DPAs have the power to monitor the lawfulness of the processing of SIS II personal data in their countries independently, as well as the exchange and further processing of supplementary information.

### CIS Regulation (1997, as amended 2008)

#### Chapter 5 – Personal-data protection

#### Article 34

1. Each CIS partner intending to receive personal data from, or include them in, the CIS shall, no later than the date of application of this Regulation, adopt national legislation, or internal rules applicable to the Commission, guaranteeing the protection of the rights and freedoms of individuals with regard to the processing of personal data.

2. A CIS partner may receive personal data from, or include them in, the CIS only where the arrangements for the protection of such data provided for in paragraph 1 have entered into force. Each Member State shall also have previously designated a national supervisory authority or authorities as provided for in Article 37.

3. To ensure the correct application of the data protection provisions of this Regulation, the Member States and the Commission shall regard the CIS as a personal data-processing system which is subject to:

- national provisions implementing Directive 95/46/EC,
- Regulation (EC) No 45/2001, and
- any more stringent provisions of this Regulation.

#### 2.1.3 Observations

**Firm legal basis**

Collective reading of all legal instruments analyzed in migration and border control cooperation has revealed that each cooperation mechanism is – first and foremost – based on a firm legal basis. Furthermore, cooperation is based on a binding and comprehensive legal instrument, most often an EU regulation. Each of these three criteria contributes to the efficiency of this type of cooperation.

By a ‘firm legal basis’, it is meant that a legal instrument must be in place at a 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 Arts 8-11 ECHR and is recurrent in the case law of the European Court of Human Rights (ECtHR). In particular, this case law refers to the interpretation of the expressions ‘in accordance with law’ or ‘prescribed by law’, occurring in Arts 8-11 ECHR (Galetta and De Hert 2014).

---

ECtHR, Olsson v Sweden (No. 1) (1988)

(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 […].

Forms of cooperation and procedures

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

By a ‘comprehensive’ legal instrument, it is meant that its content deals with all or nearly all elements or aspects of a given type of cooperation. Just a quick look at a table of contents of any legal instrument in the field reveals its comprehensive character.

SIS II Decision (2007)

Table of contents

CHAPTER I – GENERAL PROVISIONS
Article 1 – Establishment and general purpose of SIS II
Article 2 – Scope
Article 3 – Definitions
Article 4 – Technical architecture and ways of operating the SIS II
Article 5 – Costs

CHAPTER II – RESPONSIBILITIES OF THE MEMBER STATES
Article 6 – National systems
Article 7 – N.SIS II Office and SIRENE Bureau
Article 8 – Exchange of supplementary information
Article 9 – Technical compliance
Article 10 – Security – Member States
Article 11 – Confidentiality – Member States
Article 12 – Keeping of records at national level
Article 13 – Self-monitoring

Article 14 – Staff training

CHAPTER III – RESPONSIBILITIES OF THE MANAGEMENT AUTHORITY

Article 15 – Operational management
Article 16 – Security
Article 17 – Confidentiality – Management Authority
Article 18 – Keeping of records at central level
Article 19 – Information campaign

CHAPTER IV – CATEGORIES OF DATA AND FLAGGING

Article 20 – Categories of data
Article 21 – Proportionality
Article 22 – Specific rules for photographs and fingerprints
Article 23 – Requirement for an alert to be entered
Article 24 – General provisions on flagging
Article 25 – Flagging related to alerts for arrest for surrender purposes

CHAPTER V – ALERTS IN RESPECT OF PERSONS WANTED FOR ARREST FOR SURRENDER OR EXTRADITION PURPOSES

Article 26 – Objectives and conditions for issuing alerts
Article 27 – Additional data on persons wanted for arrest for surrender purposes
Article 28 – Supplementary information on persons wanted for arrest for surrender purposes
Article 29 – Supplementary information on persons wanted for arrest for extradition purposes
Article 30 – Conversion of alerts on persons wanted for arrest for surrender purposes or extradition purposes
Article 31 – Execution of action based on an alert on a person wanted for arrest with a view to surrender or extradition

CHAPTER VI – ALERTS ON MISSING PERSONS

Article 32 – Objectives and conditions for issuing alerts
Article 33 – Execution of the action based on an alert

CHAPTER VII – ALERTS ON PERSONS SOUGHT TO ASSIST WITH A JUDICIAL PROCEDURE

Article 34 – Objectives and conditions for issuing alerts
Article 35 – Execution of the action based on an alert

CHAPTER VIII – ALERTS ON PERSONS AND OBJECTS FOR DISCREET CHECKS OR SPECIFIC CHECKS

Article 36 – Objectives and conditions for issuing alerts
Article 37 – Execution of the action based on an alert

CHAPTER IX – ALERTS ON OBJECTS FOR SEIZURE OR USE AS EVIDENCE IN CRIMINAL PROCEEDINGS

Article 38 – Objectives and conditions for issuing alerts
Article 39 – Execution of the action based on an alert

CHAPTER X – RIGHT TO ACCESS AND RETENTION OF ALERTS

Article 40 – Authorities having a right to access alerts
Article 41 – Access to SIS II data by Europol
Article 42 – Access to SIS II data by Eurojust
Article 43 – Scope of access
Article 44 – Retention period of alerts on persons
Article 45 – Retention period of alerts on objects

CHAPTER XI – GENERAL DATA PROCESSING RULES

Article 46 – Processing of SIS II data
Article 47 – SIS II data and national files
Article 48 – Information in case of non-execution of alert
Article 49 – Quality of the data processed in SIS II
Article 50 – Distinguishing between persons with similar characteristics
Article 51 – Additional data for the purpose of dealing with misused identities
Article 52 – Links between alerts
Article 53 – Purpose and retention period of supplementary information
Article 54 – Transfer of personal data to third parties
Article 55 – Exchange of data on stolen, misappropriated, lost or invalidated passports with Interpol

CHAPTER XII – DATA PROTECTION

Article 56 – Processing of sensitive categories of data
The idea here should be not to make the cooperation process unnecessarily complicated or too prescriptive, but rather to be exhaustive as to what supervisory authorities might come across during the cooperation process, thus contributing to legal certainty.

Dariusz Kloza and Anna Mościbroda, “Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law”, op. cit. (2014)\textsuperscript{40}

[...]
effective enforcement cooperation between DPAs cannot take place without comprehensively defining its forms and procedures. Although the current arrangements for DPA cooperation often define forms of cooperation and procedures—ranging from the designation of contact points, notification about investigations, mutual assistance, and grounds for refusal, to time-frames, linguistic issues, and costs of such assistance—there is often a lack of comprehensive rules dealing with all these issues. This is a good starting point, but procedures described in greater detail and a common understanding of key terms and notions are lacking. The only two exceptions are probably the APEC Cross-border Privacy Enforcement Agreement and the recent Dutch-Canadian MoU.

This reflection on the 'comprehensiveness' of any cooperation arrangement lead to a long lasting debate as to the table of contents of a possible legal instrument on cooperation among supervisory authorities in the area of data privacy law. To that end, De Hert and Boulet (2014, 41–43) made an attempt to identify and categorise – as they call – ‘best elements in a cooperation instrument for DPAs’.

Paul De Hert and Gertjan Boulet, Legal reflections for further improving cooperation between data protection authorities, Deliverable D2.2 of the PHAEDRA project, Brussels (2014)\textsuperscript{41}

Annex 2
Recommended classification of aims and best elements in a cooperation instrument for DPAs

Below, we propose a classification of the aims and best elements in Deliverable 2.1 in four categories that could frame a potential cooperation instrument for DPAs: scope of application, substantive, procedural, and non-legal provisions. [...]

1. Aims
   1.1. Prevention of violations of privacy and data protection laws
   1.2. Standard setting
      1.2.1. Mutual recognition of binding corporate rules
      1.2.2. Coordination of policies in the enforcement of privacy and data protection laws
      1.2.3. Coordination of enforcement methods

\textsuperscript{40} Original footnotes omitted. Emphasis ours.
\textsuperscript{41} Original footnotes omitted.
1.2.4. Determination of sanctions for privacy and data protection offences
1.3. Enforcement of privacy and data protection laws
1.4. Assistance between DPAs
1.5. Raising Awareness

2. Scope
2.1. Compulsory nature of cooperation mechanisms
2.2. Definitions
2.3. Scope of application
   2.3.1. Scope of application rationae materiae
   2.3.2. Scope of application rationae personae
2.4. Forms of cooperation
   2.4.1. Common elements for various aims of cooperation
      2.4.1.1. Monitoring privacy and data protection laws in other countries
      2.4.1.2. Sharing of standards and information
      2.4.1.3. Trainings & staff exchanges
      2.4.1.4. Possibility to carry out projects to improve cooperation
   2.4.2. Enforcement cooperation
      2.4.2.1. Mutual legal assistance
      2.4.2.2. Parallel or joint investigations
      2.4.2.3. Mutual recognition
2.5. Allowing spontaneous information exchanges
2.6. Categories of information
   2.6.1. Common elements for various aims of cooperation
   2.6.2. Enforcement cooperation
      2.6.2.1. Information on investigative techniques
      2.6.2.2. Information about the procedure before a DPA
      2.6.2.3. Factual information
2.7. Other elements for enforcement cooperation
   2.7.1. International nature of an enforcement case
   2.7.2. Phase of an enforcement case
   2.7.3. Type of infringement
   2.7.4. Actor of infringement

3. Substantive provisions
3.1. Obligation to safely transmit and safeguard data
3.2. Other elements for enforcement cooperation
   3.2.1. Clarification of the limitation grounds for cooperation between DPAs
      3.2.1.1. Principle of double legality
      3.2.1.2. Substantially similar conduct
      3.2.1.3. National laws
      3.2.1.4. Personal data
      3.2.1.5. Refusal grounds
      3.2.1.6. Confidentiality
      3.2.1.7. Principle of proportionality
      3.2.1.8. Consent of the data subject
      3.2.1.9. Safeguards for the use of data
   3.2.2. Prioritization of matters

4. Procedural provisions
4.1. Independence of DPAs
4.2. Obligation to designate an authority for the purposes of cooperation
4.3. Legal basis for cooperation
4.4. Best efforts to resolve disagreements
4.5. Forms for cooperation requests
4.6. International cooperation units
4.7. Development of an E–platform for cooperation between DPAs
4.8. Tools for evaluation and sanctions
   4.8.1. Common element for various aims of cooperation
   4.8.2. Enforcement
4.9. Tools for further cooperation
   4.9.1. Common elements for various aims of cooperation
   4.9.2. Enforcement cooperation
4.10. Other elements for enforcement cooperation
   4.10.1. Clarification of the cross-border investigatory powers of DPAs
4.10.2. Intervention of DPAs in foreign courts
4.10.3. Prioritization of matters
4.10.4. One-stop shop
4.10.5. Consistency mechanism
4.10.6. Referral of complaints
4.10.7. Coordination body for enforcement cooperation
4.10.8. Tools for evaluation

5. Non-legal provisions
   5.1. Budget for cooperation
   5.2. Sharing costs

(b) Extraterritoriality

Dariusz Kloza and Antonella Galetta, Towards efficient cooperation between supervisory authorities in the area of data privacy law, op. cit. (2015)

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.

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.

Perhaps the most pertinent example of extraterritorial jurisdiction is the Schengen system. If a person is presumed to have taken part in an extraditable criminal offence and he has moved from one Schengen state to another, the former state can keep conducting investigations on him “on the ground” and beyond its national borders, as long as authorised by the latter. Furthermore, for a number of violent and serious

42 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)
crimes, in a situation of urgency, such an authorisation is initially replaced by mere notification (Galetta and Kloza 2016, 495–498).

**Constitution Implementing the Schengen Agreement (1990)**

**Article 40**

1. Officers of one of the Contracting Parties who, as part of a criminal investigation, are keeping under surveillance in their country a person who is presumed to have participated in an extraditable criminal offence shall be authorised to continue their surveillance in the territory of another Contracting Party where the latter has authorised cross-border surveillance in response to a request for assistance made in advance. Conditions may be attached to the authorisation.

On request, the surveillance will be entrusted to officers of the Contracting Party in whose territory this is carried out.

The request for assistance referred to in the first subparagraph must be sent to an authority designated by each of the Contracting Parties and empowered to grant or to pass on the requested authorisation.

2. Where, for particularly urgent reasons, prior authorisation cannot be requested from the other Contracting Party, the officers carrying out the surveillance shall be authorised to continue beyond the border the surveillance of a person presumed to have committed criminal offences listed in paragraph 7, provided that the following conditions are met:

(a) the authority of the Contracting Party designated under paragraph 5, in whose territory the surveillance is to be continued, must be notified immediately, during the surveillance, that the border has been crossed;
(b) a request for assistance submitted in accordance with paragraph 1 and outlining the grounds for crossing the border without prior authorisation shall be submitted immediately.

Surveillance shall cease as soon as the Contracting Party in whose territory it is taking place so requests, following the notification referred to in (a) or the request referred to in (b) or, where authorisation has not been obtained, five hours after the border was crossed.

3. The surveillance referred to in paragraphs 1 and 2 shall be carried out only under the following general conditions:

(a) The officers carrying out the surveillance must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions of the competent local authorities.
(b) Except in the situations outlined in paragraph 2, the officers shall, during the surveillance, carry a document certifying that authorisation has been granted.
(c) The officers carrying out the surveillance must at all times be able to prove that they are acting in an official capacity.
(d) The officers carrying out the surveillance may carry their service weapons during the surveillance save where specifically otherwise decided by the requested Party; their use shall be prohibited save in cases of legitimate self-defence.
(e) Entry into private homes and places not accessible to the public shall be prohibited.
(f) The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance.
(g) All operations shall be the subject of a report to the authorities of the Contracting Party in whose territory they took place; the officers carrying out the surveillance may be required to appear in person.
(h) The authorities of the Contracting Party from which the surveillance officers have come shall, when requested by the authorities of the Contracting Party in whose territory the surveillance took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings. […]

7. The surveillance referred to in paragraph 2 may only be carried out where one of the following criminal offences is involved:

- murder,
- manslaughter,
- rape,
- arson,
- forgery of money,

– aggravated burglary and robbery and receiving stolen goods,
– extortion,
– kidnapping and hostage taking,
– trafficking in human beings,
– illicit trafficking in narcotic drugs and psychotropic substances,
– breach of the laws on arms and explosives,
– wilful damage through the use of explosives,
– illicit transportation of toxic and hazardous waste.

(c) Use of technology

The broad goals of EU free movement, realized both by Schengen and Dublin systems, nowadays are – at the functional level, realised – to a large extent – by the use of technology, and in particular of ICTs. This is a significant change from how border control looked some few decades ago. Nowadays EU borders run on technology (including infrastructure) on which the flow of information depends. However, the almost entire dependence of the EU migration and border control on technologies has been highly criticised (cf. e.g. Brom and Besters 2010, 445–470).


Just a few decades ago, border control in Europe was a matter of a barrier and a passport. When passing the border, an officer would check your passport and look you in the eyes with a stern face to find out if there is anything suspicious. Information technology has transformed this picture completely. Today, information systems make the difference: being admitted to the European Union or not. With the introduction of the Schengen Information System in 1995, the first European database was implemented for the purpose of controlling the migration flow. That particular event marks the transformation of European borders into digital borders enabling ‘mass surveillance’. The introduction of information technology has set the stage for what can be called the digitalization of the European migration policy. By adding biometric data, these digital borders are even transformed into ‘biometric borders’.

The Schengen Information System has simplified the sharing of information among Member States. Having information at one’s fingertips, the efficiency and effectiveness of border control has improved. In addition to the Schengen Information System, a database was implemented to register asylum applications: Eurodac. This database was equipped with a new feature: fingerprints for the purpose of identification. With these two information systems in place, the European Commission has expressed the aim to set up a single Union information system. In trying to realize this aim, the European Commission is developing new information systems and supports the synergy between the existing ones. Without doubt, the events of 9/11 have accelerated this process of digitalization, but, as defended in an earlier study of the Rathenau Institute, these developments were initiated already before the terrorist attacks.

The process of digitalization of the European migration policy displays a great trust in information technology. And it remains to be seen whether this trust pays off. Some critics […] claim that there is an ‘untested belief’ in security technologies as the ultimate solution for any threat the EU might face. Actually, the European migration policy is turned into a kind of ‘test lab’ for new technologies:

(…) it is important to recognize that many of its [the EU’s] most controversial systems – finger- printing, ID cards, populations databases, “terrorist” profiling, travel surveillance and so on – have been (and are still being) “tested” on migrants and refugees or otherwise legitimized at the border. Acquiescence to these controls and indifference to the suffering of migrants and refugees at the hands of “Fortress Europe” has paved the way for their use in domestic security scenarios.

[…] We will argue that the trust in information technology affects the outline and development of the European migration policy. We will claim that information technology is ‘greedy’: it elicits a dynamic of its own in which the political ends become to depend heavily on the technical means. As a consequence, the European migration policy runs the risk of being stuck in a ‘digital fix’, i.e. a technological fix focusing on information technology.

44 For the debate on the changes on EU external borders, cf. e.g. (Stănculescu 2012, 23–31) and (Bigo 2014).
45 Original footnotes omitted.
The basic architecture of SIS II, VIS and Eurodac consists of national databases linked to a central system set at EU level; they are connected among each other by a communication infrastructure.

For example, **SIS II** consists of two main databases, namely a central system (Central SIS II) and a national system (N.SIS II), which is established in each Schengen state and communicates with Central SIS II. Moreover, there is a communication infrastructure between Central SIS and N.SIS that allows the exchange of encrypted data. Whenever a set of data is entered into SIS, it generates an alert. N.SIS II systems contain information entered, updated and deleted by national authorities at national level, whereas the Central SIS II is basically a repository of all SIS II alerts. Information about a person or an object entered into the N.SIS systems is sent by the N.SIS system itself to the Central SIS. It follows that information contained in Central SIS is consistent with that of the N.SIS systems. In addition, the Central SIS system provides functionalities for ensuring synchronisation and consistency of national copies as well as their restoration. As a result, national authorities in Schengen states have access to and can exchange up-to-date information in real time and on a permanent basis, using secure channels.

**VIS** consists of national systems established in each Member State, a central IT system and a communication infrastructure that connects the central system to the national systems via the national interface. Information that is entered in national systems by consular authorities of each Member State is transferred to the central IT system which collects all requests for visas introduced at national level. Moreover, the architecture of VIS allows national authorities in Member States to check whether a certain applicant introduced the same request for a visa in another Member State and whether it was issued, refused, annulled revoked or extended. As a consequence, VIS prevents “visa-shopping” practices while at the same time smoothing administrative procedures for consular and border control authorities in Member States. Each Member States is responsible for the development, organisation, management, operation and maintenance of its national system. Also, each Member State is obliged to ensure that its consular authorities have access to the national system.

Other national authorities (i.e. those responsible for border control and asylum) as well as EU institutions and bodies can access VIS. Europol can consult VIS “for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences”.

Concerning **Eurodac**, Member States are obliged to transmit the fingerprints of asylum seekers and illegal immigrants to the Central Unit “as soon as possible and no later than 72 hours from the date of apprehension” supplemented by:

- the Member State who enters those data;
- the reference number it uses;
- the gender of the asylum seeker or illegal immigrant;
- the date on which the fingerprints were taken;
- the date on which the data were transmitted to the Central Unit and were entered in the central database.

Once all these data are transmitted to the Central Unit, they are compared by the Central Unit itself with the fingerprint data transmitted by other Member States and that are already stored in the central database. In turn, the Central Unit transmits the result of this comparison immediately to the Member State who entered the data into the system. It is the responsibility of each Member State who forwards data to the Central Unit to make sure that they have been recorded lawfully and are accurate. Hence, Member States should amend, correct or erase them, should the need arise. Europol can access Eurodac data.

**CIS** consists of a central database facility that is accessible via terminals in each Member State and at the Commission. Direct access to the data contained in the CIS is allowed to competent national authorities designated in each Member State on the basis of a list sent by them to the Commission. These national authorities are normally customs administrations but other authorities may also be included. In turn, the Commission informs Member States about the Commission departments authorised to have access to the CIS. In addition, the Council may decide to permit access to the CIS by international or regional organisations on the basis of specific arrangements.

**(d) Time**

The use of technology permits secure (i.e. encrypted), easy, continuous, reliable, real-time and up-to-date access to information for multiple actors.
(e) Multilingualism

i) General observations

A few observations on European languages shall precede the deliberations on the optimal choice of them for the use in cooperation. Generally speaking, there are 24 official languages of the EU, more than 60 indigenous regional and minority languages as well as many non-indigenous languages spoken by migrant communities. EU languages are written in 3 scripts: Latin, Greek and Bulgarian Cyrillic. The Union asserts that it is in favour of linguistic diversity; cf. Art 22 CFR and in Art 3(3) TEU. It is a principle that all EU institutions can be addressed in any of the official languages and the petitioner will receive a reply in the official EU language of her choice. Furthermore, it is a principle of fair trial (due process) in criminal cases that an individual is addressed “in a language which he understands”. However, in any areas of cooperation in the EU, it is neither feasible nor pragmatic to use all official languages and the choice thereof would always be considered political. In addition, both translation and interpretation takes time and their cost can be significant.

There are a number of possible patterns to follow, for instance:

(a) the choice of a limited number thereof: for example, European Patent Office (EPO) works in English, French and German; the Office for Harmonization in the Internal Market (OHIM) works in five languages;
(b) the use of a ‘bridging language’: for example, the CJEU, in its internal work, choses one official language to bridge all the translations and interpretation, but the final outcome, i.e. the judgement, is always eventually translated to all languages;
(c) the choice of the language: for example, people can agree on a way to communicate, a principle well known from contract law; However, Krepelka observed that Europeans have little knowledge of foreign languages and enhanced education in last decades has limited success. Only few European countries have population with knowledge of foreign languages generally perceived satisfactory (2012, 101);
(d) the use of single language mandated by law: for example, “the International Civil Aviation Organization, pilots of planes on international flights are expected to communicate either in their own language or in English at request of air traffic controllers” (Krepelka 2012, 114);
(e) the use of automatic translation, to the extent ever possible.

Furtherer possibilities are being explored throughout the present report.

ii) Multilingualism in migration and border control cooperation

When it comes to migration and border control cooperation, it is first observed that neither translation nor interpretation is necessary in all instances. Multilingualism does not constitute an obstacle to cooperation among Member States in the cases of SIS II, VIS and Eurodac. The alphanumeric nature and type of information processed by these systems does not raise any linguistic issue (Brouwer 2008).


During the negotiations, the participating officials made it clear that the SIS should make it possible to identify persons or goods searched by the national authorities of one of the Schengen states on an easy and fast manner, without excessively hampering the circulation of travellers crossing external borders. Therefore, the SIS would have to contain only the necessary information for the requested action and the SIS terminals would have to be

46 Cf. the question of languages to be used for the European patent, which was concluded with Spain and Italy withdrawing.
48 The example of Google Translate as a tool for machine translation of a general application is rather well known. Yet there are areas that might require specific, highly specialised automatic translation. To that end, for example, the EU has co-funded under FP7, a commercial development project PLuTO [Patent Language Translations Online; 2010-13; http://www.pluto-patenttranslation.eu] whose aim has been to “eliminate the language barriers that exist worldwide in the provision of multilingual access to patent information”. The project later on turned into a commercial platform under the label of “IPTranslator” (cf. http://iptranslator.com).
49 Original footnotes omitted.
easy accessible, comparable to the national police systems already used in the different Schengen countries. An officer checking the system should also be clearly informed about the actions to be taken. The problem of language and the use of different concepts was solved by the introduction of a structure of limited categories of data to be stored in the system, clearly describing the actions to be taken each time a check on the SIS resulted in a ‘hit’. One of the major advantages of this system would be that it resolved the normal problems of translation, since each recipient could deduce all the relevant information from the location of the data in the system.

Specific arrangements to avoid linguistic problems are then established in the context of CIS in which translation should normally be provided by the Member State that introduces a request for notification.

**The CIS Regulation (1997)**

**Article 6**

1. At the request of the applicant authority, the requested authority shall, while observing the rules in force in the Member State in which it is based, notify the addressee or have it notified of all instruments or decisions which emanate from the administrative authorities and concern the application of customs or agricultural legislation.

2. Requests for notification, mentioning the subject of the instrument or decision to be communicated, shall be accompanied by a translation in the official language or an official language of the Member State in which the requested authority is based, without prejudice to the latter’s right to waive such a translation.

**Convention implementing the Schengen Agreement (1990)**

**CHAPTER 4**

**APPORTIONMENT OF THE COSTS OF THE SCHENGEN INFORMATION SYSTEM**

**Article 119**

1. The costs of installing and operating the technical support function [...], including the cost of lines connecting the national sections of the Schengen Information System to the technical support function, shall be borne jointly by the Contracting Parties. Each Contracting Party's share shall be determined on the basis of the rate for each Contracting Party applied to the uniform basis of assessment of value added tax within the meaning of Article 2(1)(c) of the Decision of the Council of the European Communities of 24 June 1988 on the system of the Communities' own resources.

2. The costs of installing and operating the national section of the Schengen Information System shall be borne by each Contracting Party individually.

**SIS II Decision (2007)**

**Article 5**

**Costs**

1. The costs of setting up, operating and maintaining Central SIS II and the Communication Infrastructure shall be borne by the general budget of the European Union.

2. These costs shall include work done with respect to CS-SIS that ensures the provision of the services referred to in Article 4(4).

3. The costs of setting up, operating and maintaining each N.SIS II shall be borne by the Member State concerned.
VIS Regulation (2008)

Article 28
Relation to the national systems

[...] 4. Each Member State shall be responsible for: [...] 
(d) bearing the costs incurred by the national system and the costs of their connection to the national interface, including the investment and operational costs of the communication infrastructure between the national interface and the national system.

Eurodac Regulation (2013)

Article 39
Costs

1. The costs incurred in connection with the establishment and operation of the Central System and the Communication Infrastructure shall be borne by the general budget of the European Union.

2. The costs incurred by national access points and the costs for connection to the Central System shall be borne by each Member State.

3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and shall be responsible for bearing its costs resulting from requests for comparison with Eurodac data for the purposes laid down in Article 1(2).

The costs of the functioning of migration and border control cooperation are split between the central budget of the EU and budgets of each Member State. The rationale for such a split follows the technical architecture of the databases at stake. They are built of a central unit and national units. Thus the EU budget covers the cost of running the former and well as of the EU-Lisa and the budgets of Member States cover the costs of running national units.

EU-Lisa Regulation (2011)

Article 32
Budget

1. The revenue of the Agency shall consist, without prejudice to other types of income, of:

(a) a subsidy from the Union entered in the general budget of the European Union (Commission section);
(b) a contribution from the countries associated with the implementation, application and development of the Schengen acquis and Eurodac-related measures;
(c) any financial contribution from the Member States.


TITLE VI – FINANCING

Article 42a

1. This Regulation is the basic act on which the financing of all Community action provided for herein is based, including:

(a) all costs of installing and maintaining the permanent technical infrastructure making available to the Member States the logistical, office automation and IT resources to coordinate joint customs operations, in particular special surveillance operations provided for in Article 7;
(b) the reimbursement of transport, accommodation and daily allowance costs of representatives of the Member States taking part in the Community missions provided for in Article 20, joint customs operations organised
by or jointly with the Commission and training courses, ad hoc meetings and preparatory meetings for
administrative investigations or operational actions conducted by the Member States, where they are
organised by or jointly with the Commission.

Where the permanent technical infrastructure referred to in point (a) is used for the purposes of the customs
cooporation provided for in Articles 29 and 30 of the Treaty on European Union, the transport,
accommodation costs and the daily allowances of the representatives of the Member States shall be borne by
the Member States;

(c) expenditure relating to the acquisition, study, development and maintenance of computer infrastructure
(hardware), software and dedicated network connections, and to related production, support and training
services for the purpose of carrying out the actions provided for in this Regulation, in particular preventing
and combating fraud;

(d) expenditure relating to the provision of information and expenditure on related actions allowing access to
information, data and data sources for the purpose of carrying out the actions provided for in this
Regulation, in particular preventing and combating fraud;

(e) expenditure relating to use of the CIS provided for in instruments adopted under Articles 29 and 30 of the
Treaty on European Union and in particular in the Convention on the use of information technology in
customs matters drawn up by the Council Act of 26 July 1995, in so far as those instruments provide that
that expenditure shall be borne by the general budget of the European Union.

2. Expenditure relating to the acquisition, study, development and maintenance of the Community components
of the common communication network used for the purposes of paragraph 1(c) shall also be borne by the
general budget of the European Union. The Commission shall conclude the necessary contracts on behalf of the
Community to ensure the operational nature of those components.

3. Without prejudice to the expenses relating to the operation of the CIS and the amounts provided for by way
of compensation pursuant to Article 40, the Member States and the Commission shall waive all claims for the
reimbursement of expenditure relating to the supply of information or of documents or to the implementation
of an administrative investigation or of any other operational action pursuant to this Regulation which are carried
out at the request of a Member State or the Commission, except as regards the allowances, if any, paid to
experts.

(g) Geographical scope

Access to the three above-mentioned databases – i.e. SIS II, VIS and Eurodac – is granted not only to the
‘main’ category of authorities whose are preoccupied with each of them. It might be also granted to
supranational- and international institutions, e.g. Europol or Interpol.

As for the goals of these migration and border control systems sometimes there is a need to resort to third
parties, such as authorities in third countries or international organizations, the legal framework explicitly
enables such a possibility.

CIS Regulation (1997)

TITLE IV – RELATIONS WITH THIRD COUNTRIES

Article 19

Provided the third country concerned has given a legal undertaking to provide the assistance required to gather
proof of the irregular nature of operations which appear to constitute breaches of customs or agricultural
legislation or to determine the scope of operations which have been found to constitute breaches of that
legislation, information obtained under this Regulation may be communicated to that third country as part of a
concerted action, subject to the agreement of the competent authorities supplying the information, in accordance
with their internal provisions concerning the communication of personal data to third countries.

The information shall be communicated either by the Commission or by the Member States as part of the
concerted action referred to in the first paragraph; in either case appropriate steps shall be taken in the third
country concerned to ensure a degree of protection equivalent to that laid down by Article 45 (1) and (2).

Article 20

1. In pursuit of the objectives of this Regulation, the Commission may, under the conditions laid down in
Article 19, conduct Community administrative and investigative cooperation missions in third countries in
coordination and close cooperation with the competent authorities of the Member States.
2. The Community missions to third countries referred to in paragraph 1 shall be governed by the following conditions:

(a) they may be undertaken at the Commission's initiative, where appropriate on the basis of information supplied by the European Parliament, or at the request of one or more Member States;
(b) they shall be carried out by Commission officials appointed for that purpose and by officials appointed for that purpose by the Member State(s) concerned;
(c) they may also, by agreement with the Commission and the Member States concerned, be carried out on behalf of the Community by officials of a Member State, in particular under a bilateral assistance agreement with a third country; in that event the Commission shall be informed of the results of the mission;
(d) mission expenses shall be paid by the Commission.

3. The Commission shall inform the Member States and the European Parliament of the results of missions carried out pursuant to this Article. [...]

**Article 22**

Member States shall notify the Commission of information exchanged within the framework of mutual administrative assistance with third countries wherever, within the meaning of Article 18 (1), it is particularly relevant to the effectiveness of customs or agricultural legislation pursuant to this Regulation and the information falls within the scope of this Regulation.
2.2 Private international law

2.2.1 Legal framework

(a) Historical

- Council regulation (EC) No 1346/2000 of 29 May 2000 on insolvency proceedings
- Council regulation (EC) No 1348/2000 of 29 May 2000 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters

(b) In force

- Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters
- Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters
Private international law


(c) Actors


2.2.2 General overview

(a) Rationale of private international law


E-commerce increases the frequency of the cross-border disputes. In such cases, at least one party is required to take the litigation abroad. Let us assume that a consumer from Prague bought a book from a seller who is an online marketplace owned by a company registered and operating in London. The price was paid, although the book has never been delivered. The consumer wants her money back. The seller left the claim not responded and hence was sued in Prague. The consumer obtained there a default pecuniary judgement in her favour. The claim remains unsatisfied. There are no seller’s assets in the Czech Republic; they are only in England.

Private international law (in common law: Conflict of Laws) deals with cases before the domestic courts which have connections with other jurisdictions (i.e. a territorial unit having its own separate system of law). Three procedural steps in the trans-border disputes include: (1) jurisdiction – which court is competent to hear the case?, (2) choice of law – what national law to apply?, and (3) recognition and enforcement – since a foreign judgement has no legal effect in a domestic legal regime. Without the recognition and enforcement, the creditor would need to start the proceedings again. In most jurisdictions, to produce such result, various intermediary proceedings (i.e. procedure of exequatur) are required.

Litigation ends when the final judgement is rendered. “It is often of little use for a party to know that a Czech court can claim jurisdiction and will apply Czech law, if the subsequent judgment cannot be enforced in a forum where the other party has assets.” It needs to be recognised (i.e. its legal effects must be extended) and enforced (executed with the assistance of the public authorities) in the respective part of the UK. (The judgement might be recognized in a foreign jurisdiction just to produce there the res judicata effect in order to prevent further proceedings between the same parties in the same case.)

(b) Development of EU private international law


1.1 ‘Judicial cooperation in civil matters’ — building bridges between the judicial systems in the EU

Private international law or — as it is called in the Treaty — ‘judicial cooperation in civil matters’ has developed into an independent and separate field of European law. […]

The principles of free movement of goods, services, capital and persons encourage the mobility of European citizens and the development of commercial activities throughout the European Union. As a result, legal practitioners find themselves increasingly faced with situations having cross-border implications and with problems and legal questions governed by EU law. […]

69 Original footnotes omitted.
1.2. Towards a genuine European area of civil justice

The rules of judicial cooperation in civil matters are based on the presumption of the equal value, competence and standing of the legal and judicial systems of the individual Member States and of the judgments of their courts and so on the principle of mutual trust in each other’s courts and legal systems. The mutual recognition of the orders of courts of the Member States is at the centre of this principle which also embraces the idea of the practice of cross-border collaboration between individual courts and court authorities. The importance of uniform rules in this field is to foster legal certainty and foreseeability in legal situations with cross-border implications: if each Member State were to individually establish which law should apply to and which court should be competent in each cross-border legal relationship and which judgments of which other Member States were to be recognised, the result would be a lack of legal certainty for citizens and enterprises both in respect to jurisdiction and the applicable law.

At the Tampere European Council on 15 and 16 October 1999 the Council had formulated the aim of the creation of a ‘genuine European area of Justice’, based on the principle that individuals and companies should not be prevented or discouraged from exercising their rights by incompatibilities between or complexities of judicial and administrative systems in the Member States. The Council established as priorities for action in this area, in particular, better access to Justice in Europe, mutual recognition of judicial decisions and increased convergence in the field of civil law.

The term judicial cooperation in civil matters originated first from the Maastricht Treaty, the Treaty on the European Union, which defined judicial cooperation in civil matters as a subject of common interest to the Member States. With the Treaty of Amsterdam, this policy of cooperation, which had hitherto been solely directed at action to be taken by the Member States, became a matter for legislative action by the institutions of the European Community. The Treaty of Lisbon refers explicitly to the principle of mutual recognition of judgments in civil matters but left the legislative competence essentially untouched. Article 81 of the Treaty on the Functioning of the European Union sets out a comprehensive list of activities which may be the subject of legislation. Many of these are familiar from the contents of the earlier Treaties but the list now mentions expressly affording effective access to justice and judicial training for members of the judiciary and the staff of the courts. Article 81 also clarifies that judicial cooperation in civil matters may include the adoption of measures for the approximation of the laws and regulations of the Member States. With the exception of measures in family law all legislation in these matters is now adopted under the ordinary legislative procedure, under which Union legislation is adopted jointly by the European Parliament and the Council as co-legislators. Family law measures are adopted under the special procedure in which the Council acts unanimously after consulting the Parliament.

---

**Treaty on the Functioning of the European Union (1957, as amended 2009)**

**TITLE V – AREA OF FREEDOM, SECURITY AND JUSTICE**

**CHAPTER 3 – JUDICIAL COOPERATION IN CIVIL MATTERS**

**Article 81**

1. The Union shall develop judicial cooperation in civil matters having cross-border implications, based on the principle of mutual recognition of judgments and of decisions in extrajudicial cases. Such cooperation may include the adoption of measures for the approximation of the laws and regulations of the Member States.

2. For the purposes of paragraph 1, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures, particularly when necessary for the proper functioning of the internal market, aimed at ensuring:

   (a) the mutual recognition and enforcement between Member States of judgments and of decisions in extrajudicial cases;
   
   (b) the cross-border service of judicial and extrajudicial documents;
   
   (c) the compatibility of the rules applicable in the Member States concerning conflict of laws and of jurisdiction;
   
   (d) cooperation in the taking of evidence;
   
   (e) effective access to justice;
   
   (f) the elimination of obstacles to the proper functioning of civil proceedings, if necessary by promoting the

---

compatibility of the rules on civil procedure applicable in the Member States;
(g) the development of alternative methods of dispute settlement;
(h) support for the training of the judiciary and judicial staff.

3. Notwithstanding paragraph 2, measures concerning family law with cross-border implications shall be established by the Council, acting in accordance with a special legislative procedure. The Council shall act unanimously after consulting the European Parliament. […]

European Commission, “Towards a true European area of Justice: Strengthening trust, mobility and growth”, press release (11 March 2014)\(^71\)

The European Commission has today outlined its vision for the future of EU justice policy. Four years after the entry into force of the Lisbon Treaty the construction of a European area of Justice has advanced in leaps and bounds. The Commission has used legislation in the area of justice to cut red tape and costs for citizens and business, to drive economic recovery and to ease the practical life of citizens making use of their free movement rights. The Commission’s objective for the future is to make further progress towards a fully functioning common European area of justice based on trust, mobility and growth by 2020.

“In the space of just a few years, justice policy has come into the limelight of European Union activity – comparable to the boost given to the single market in the 1990s. We have come a long way, but there is more to do to develop a true European area of Justice,” said Vice-President Viviane Reding, the EU’s Justice Commissioner. “Building bridges between the different justice systems means building trust. A truly European Area of Justice can only work optimally if there is trust in each other’s justice systems. We also have to focus on two other challenges: the mobility of EU citizens and business in an area without internal borders, and the contribution of EU justice policy to growth and job creation in Europe.”

[…] In the justice area, the Commission identifies three key challenges: enhancing mutual trust, facilitating mobility, and contributing to economic growth.

- **Trust.** Mutual trust is the bedrock upon which EU justice policy should be built. EU instruments such as the European Arrest Warrant or rules on conflict of laws issues between Member States require a high level of mutual trust between justice authorities from different Member States. While the EU has laid important foundations for the promotion of mutual trust, it needs to be further strengthened to ensure that citizens, legal practitioners and judges fully trust judicial decisions irrespective of in which Member State they have been taken. […]

### 2.2.3 Observations

(a) **Mutual trust**

We have observed on numerous occasions – as it is mentioned in a preamble to almost every legal instrument in the area – that judicial cooperation in civil and commercial matters in the EU is based on the principle of mutual trust, both in the legal systems of each EU Member State, in the judicial authorities therein, and their actions. In other words, the EU private international law (PIL) is based on “the presumption of the equal value, competence and standing of the legal and judicial systems of the individual Member States and of the judgments of their courts” (European Judicial Network in civil and commercial matters 2014).

The notion of mutual trust implies, *prima facie*, a ‘firm belief in the reliability, truth, or ability’\(^72\) of counterpart judicial systems, authorities and their actions. Both EU Member States and the institutions trust each other that decisions made in one EU Member State and/or by an EU institution or body adhere to substantive and procedural standards set forth and there is no need to verify that. The role of trust is that it reduces the necessity for control (Weller 2015). In result, this mutual trust has gradually allowed to treat judicial and extra-judicial decisions issued in one Member State as they were rendered in the receiving Member State as their own.

---

\(^{71}\) IP/14/233.

\(^{72}\) Oxford Dictionary of English.
The eminent German sociologist Niklas Luhmann describes trust as “confidence in one’s own expectations to other persons’ behaviour”, and this confidence constitutes “an elementary fact of social life”. Trust in the reliance of one’s own expectations reduces the complexity of life with all its incidents and possibilities. Trust is a behaviour to reduce complexity to the degree where decisions about present alternatives of actions can be taken with a view to the future. However, “[w]here control is guaranteed, there is no need for trust”. This is where the law comes in. Law provides for certainty by control. To the extent the law is “strong” in the sense that it reliably stabilises expectations, trust is of reduced relevance. Thus, from a sociological viewpoint, law and trust are functionally equivalent. The policy decision for rule-makers therefore is how to strike the balance between law and trust. And this is exactly one of the central policy questions for rule-making in judicial cooperation between states as well. This question arises, first and foremost, on the level of recognition of foreign judicial acts, in particular of foreign judgments. Secondly, to a certain degree the question plays a role in the conflict of laws.

European Court of Human Rights, Avotinš v Latvia (2014)73

49. The Court notes that, according to the Preamble to the Brussels I Regulation, that instrument is based on the principle of “mutual trust in the administration of justice” in the European Union, which implies that “the declaration that a judgment is enforceable should be issued virtually automatically after purely formal checks of the documents supplied, without there being any possibility for the court to raise of its own motion any of the grounds for non-enforcement provided for by this Regulation” (see paragraph 24 above). In that connection the Court reiterates that the observance by the State of its legal obligations arising out of membership of the European Union is a matter of general interest (see Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi cited above, §§ 150-51, and Michaud v. France, no. 12323/11, § 100, ECHR 2012). […] However, this mutual trust has proven not to be unlimited. On the one hand, both the EU institutions and the Member States have been gradually realising that not all legal systems and judicial authorities in the EU have – in practice – equal standing. This question of standing predominantly concerns problems with quality, efficiency and independence of national judicial systems as well as citizens’ trust in their own national juridical systems.

On the other hand, the EU PIL has progressively realised that legal and cultural differences exist between the EU Member States and that the judicial cooperation in civil and commercial matters could function only if these were accommodated to a reasonable extent. While there is a general trend to simplify the civil procedure, and the abolition of exequatur is perhaps the most prominent example thereof, there often still exist some grounds for refusal of recognition and enforcement. Such grounds are usually of twofold nature. The first one is “political”, acknowledging the sovereignty of a receiving jurisdiction, whose public order might not accept a given judgment. The second has to do with fundamental rights and the principle of due process in particular, where res iudicata (claim preclusion) forbids to recognize the judgment if the case has been already closed. While nobody would question the due process clauses, the grounds for refusal are more delicate. For example, while the Brussels I Regulation (recast) still maintains ordre public as a ground for refusal [Art 45(1)(a)], no such provision can be found e.g. in the European Enforcement Order Regulation. Its Art 21 concerns only due process.

This exercise to balance ‘trust’ and ‘control’ – as Weller (2015) puts it – has to be welcome. In his evaluation of the functioning of the mutual trust principle in the EU PIL, this author proposes to extend the refusal catalogue to, inter alia, manifest errors in law.

We will observe a similar trend in the development of criminal justice cooperation (cf. Sect. 2.5).

73 Judgement of 25 February 2014, application no 17502/07.

[...] according to the November 2013 Eurobarometer on “Justice in the European Union”, the majority of EU citizens believe that there are large differences between national judicial systems in terms of quality, efficiency and independence, and a considerable number of EU citizens do not even trust their own national justice system. In the context of the second Judicial Scoreboard of 2014, the Commission found that the judicial independence in the Member States of Hungary, Romania, Bulgaria and Slovakia as perceived by the people is below 3 out of a maximum value of 7 with Slovakia at the lowest rank, and Slovakia even turned out to have fallen further back, from nearly 3 to only 2.5. After the first Judicial Scoreboard in 2013, the Council had already defined country-specific recommendations in the area of justice in respect of ten Member States concerning deficiencies in independence, quality and efficiency of their justice systems or to further strengthen the judiciary. Apparently, trust – and in particular mutual trust – is reality only to a limited degree. […]

(d) Challenging the normative system by “systemic deficiencies” in a Member State

In order to integrate these challenges into the normative system of mutual trust, a convincing balance between (far-reaching) trust and (residual) control needs to be achieved. In the long run, only such a balance will uphold and enhance real mutual trust amongst the Member States.

(i) Express public policy clause […]
(ii) Implied public policy control […]
(iii) Révision au fond for manifest errors of law […]
(iv) The European Union needs to trust its Member States […]

---

Brussels I Regulation (recast) (2012)

[Recital 26]
Mutual trust in the administration of justice in the Union justifies the principle that judgments given in a Member State should be recognised in all Member States without the need for any special procedure.

[Recital 27]
For the purposes of the free circulation of judgments, a judgment given in a Member State should be recognised and enforced in another Member State even if it is given against a person not domiciled in a Member State.

Article 36
1. A judgment given in a Member State shall be recognised in the other Member States without any special procedure being required.

Article 39
A judgment given in a Member State which is enforceable in that Member State shall be enforceable in the other Member States without any declaration of enforceability being required.

Article 40
An enforceable judgment shall carry with it by operation of law the power to proceed to any protective measures which exist under the law of the Member State addressed.

[…]

Article 45
1. On the application of any interested party, the recognition of a judgment shall be refused:

(a) if such recognition is manifestly contrary to public policy (ordre public) in the Member State addressed;
(b) where the judgment was given in default of appearance, if the defendant was not served with the document which instituted the proceedings or with an equivalent document in sufficient time and in such a way as to enable him to arrange for his defence, unless the defendant failed to commence proceedings to challenge the judgment when it was possible for him to do so;
(c) if the judgment is irreconcilable with a judgment given between the same parties in the Member State addressed;
(d) if the judgment is irreconcilable with an earlier judgment given in another Member State or in a third State
involving the same cause of action and between the same parties, provided that the earlier judgment fulfills the conditions necessary for its recognition in the Member State addressed; […]

**Article 52**

Under no circumstances may a judgment given in a Member State be reviewed as to its substance in the Member State addressed.

Mutual trust is of equal importance for private international law and for cross-border cooperation in the area of data privacy law. While the GDPR sets forth the new *modus operandi* of such cooperation inside the EU, in particular by obliging national DPAs to cooperate and by establishing the one-stop-shop mechanism as well as procedures for consistent decision-making, among others, it correspondingly implies that each DPA should trust its counterparts in the manner similar to the mutual trust principle observed in the EU PIL. It has already been observed that a first prerequisite to establish mutual trust among DPAs is to treat each other as peers. “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” (Kloza and Galetta 2015, 16).

However, it cannot be excluded that the daily work of the EDBP would be confronted with the problem of mutual trust. We see that this development is likely to raise similar concerns as in the area of EU PIL, these pertaining to equal standing of each DPA, which in practice might be controversial, as well as to grounds for refusal.

**(b) Gradual development**

It could be well argued that the entire process of European integration has been gradual. It all stated in 1950s with a belief that “the European integration would be best furthered by focusing initially on discrete economic sectors which could be managed efficiently and technocratically by supranational institutions, away from the fray of politics” and the political dimension emerged later on (Craig and de Búrca 2008; emphasis added). The process of European integration itself is an experiment and as such it should be conducted carefully, step-by-step.

A similar observation might be made about the development of the EU PIL (cf. e.g. Svantesson 2016, 321–422). First, the initial areas of harmonisation have been chosen carefully and selectively, originally focusing solely on the smoothing of the functioning of the internal market. Therefore the first area targeted was jurisdiction and recognition and enforcement of judgements in civil and commercial matters, as illustrated by the 1968 Brussels Convention. This harmonisation initially was achieved at an intra-governmental level, i.e. by means of an international treaty signed under the auspices of the then-European Economic Community.

However, as the European integration process progressed, a need was observed to both enhance the substantive scope of EU PIL as well as – with a view of increasing efficiency – to enhance legislative powers of the EU in this area, i.e. to harmonise by supranational means. The Amsterdam Treaty (1997) made the EU PIL the competence of the European Community (i.e. former first pillar) with qualified majority voting, short of family matters, where unanimity was maintained in the Council of Ministers. This speeded up the development of the EU PIL and multiple instruments stated appearing after 2001.

Merely looking at the “history” of the *exequatur* in the EU PIL gives an overview of this gradual development. The 1968 Brussels Convention, replaced in 2000 by Brussels I Regulation offered automatic recognition of judgements, i.e. producing of legal effects, but enforcement still required intermediary proceedings. In 2004, with the arrival of the European Enforcement Order, the procedure of *exequatur* was abandoned within its scope of application, i.e. uncontested claims. In 2006 this thinking was extended to European Payment Order and in 2007 – to European Small Claims Procedure. Upon evaluations of all these instruments, the recast of Brussels I Regulation abandoned the *exequatur* altogether. This move could question the *ratio legis* for other instruments introduced earlier. Yet, generally speaking, the creditor still maintains the choice of a method – between all-purpose Brussels I Regulation and specific instruments (i.e. EEO, EPO and ESCP) – to obtain satisfaction to this debt.

---

74 Exequatur is a decision by a court or other competent authority allowing the enforcement in that country of a judgment, arbitral award, authentic instrument or court settlement given in another jurisdiction.
Figure 3: Overview of the selected enforcement procedures in the EU (Kloza 2010, 30)

It is also worth noting that since its inception till the Lisbon Treaty (2007), the EU PIL was meant to be developed gradually. Art 61 of the pre-Lisbon EC Treaty directly spoke about establishing “progressively an area of freedom, security and justice” (emphasis added), where the EU PIL constituted a part thereof. This was abandoned after Lisbon and the current wording of Art 81 TFEU speaks about “the Union [that] shall develop judicial cooperation in civil matters having cross-border implications”.


[…] Another argument [for the path of gradual adoption] is that the courts have only recently begun to apply and interpret many instruments of the framework. It seems appropriate to wait and see how the courts of the Member States and of the CJEU apply and interpret these new instruments on private international law.

The novel, experimental – and thus to some extent controversial – cooperation mechanisms in data privacy law should be introduced gradually. In the framework of GDPR, especially with one-stop-shop mechanism and procedures for consistent decision-making, a revision clause should be introduced. These mechanisms should be evaluated after, say five years, and if they do not live up to the expectations vested therein, they should be revised or abandoned altogether.

It is noteworthy that the notion of ‘personal data protection’ has entered the EU Treaties in a similar manner (cf. González Fuster 2014).

(c) Multilingualism

Cooperation within the EU PIL often necessitates dealing not only with alphanumeric data, but also with documents (e.g. judgements) and procedures (e.g. hearings) in multiple languages. While it was not expected that this would raise any troubles with Member States sharing official languages, e.g. between Germany and Austria or Belgium and France, it was deemed necessary to solve linguistic problems with other jurisdictions.

Similarly to cooperation in migration and border control, we observe that in all EU PIL instruments the problem of multiple languages was solved at the supranational level. This ultimately closed debates among Member States whether their national systems would recognize and give effect to legal documents

and procedures in other languages. However, this was done not without leaving some leeway to the Member State. For example, in case of the European Enforcement Order (EEO), each Member State communicated to the European Commission the languages other than their official ones, in which it would recognize and give effect to the EEO certificate [cf. Art 20(2)(c)].

Second, we observe that the EU PIL functions predominantly on certificates. Each instrument establishing each procedure – be it Brussels I Regulation or EEO – offers a set of compulsory certificates to be issued by a judicial authority in the Member State of origin. These certificates contain predominantly alphanumeric data and thus they eliminate the need for their translation. It is only if the non-Latin script is used, as with Bulgarian or Greek languages, when transliteration is necessary. Translation of the whole documentation is limited to the exceptional circumstances.

The use of certificates and – generally speaking – forms with alphanumeric information only is not a novelty in the EU. The most well known example of their use is the template for a driving license in the EU.

### European Enforcement Order Regulation (2004)

**Article 20**

2. The creditor shall be required to provide the competent enforcement authorities of the Member State of enforcement with:

(a) a copy of the judgment which satisfies the conditions necessary to establish its authenticity; and

(b) a copy of the European Enforcement Order certificate which satisfies the conditions necessary to establish its authenticity; and

(c) where necessary, a transcription of the European Enforcement Order certificate or a translation thereof into the official language of the Member State of enforcement or, if there are several official languages in that Member State, the official language or one of the official languages of court proceedings of the place where enforcement is sought, in conformity with the law of that Member State, or into another language that the Member State of enforcement has indicated it can accept. Each Member State may indicate the official language or languages of the institutions of the European Community other than its own which it can accept for the completion of the certificate. The translation shall be certified by a person qualified to do so in one of the Member States.

### Brussels I Regulation (recast) (2012)

**Article 37**

1. A party who wishes to invoke in a Member State a judgment given in another Member State shall produce:

(a) a copy of the judgment which satisfies the conditions necessary to establish its authenticity; and

(b) the certificate issued pursuant to Article 53.

2. The court or authority before which a judgment given in another Member State is invoked may, where necessary, require the party invoking it to provide, in accordance with Article 57, a translation or a transliteration of the contents of the certificate referred to in point (b) of paragraph 1. The court or authority may require the party to provide a translation of the judgment instead of a translation of the contents of the certificate if it is unable to proceed without such a translation. […]

**Article 53**

The court of origin shall, at the request of any interested party, issue the certificate using the form set out in Annex I. […]

**Annex I**

---


77 Only the first page is reproduced here.
The exchange of information for the purposes of cooperation in data privacy law should rely – to the highest possible extent – on the use of ‘alphanumeric forms’ for exchanging of information. This would constitute the first step e.g. in feeding enforcement databases. Only when the need to exchange textual documents, i.e. intermediate decisions or so, arrives, then the translators should step in.
2.3 Consumer protection cooperation

2.3.1 Legal framework

Past


In force

- Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain\(^{79}\)
- Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration\(^{80}\)
- Commission Implementing Regulation (EU) 2015/1051 of 1 July 2015 on the modalities for the exercise of the functions of the online dispute resolution platform, on the modalities of the electronic complaint form and on the modalities of the cooperation between contact points provided for in Regulation (EU) No 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes\(^{85}\)

2.3.2 General overview

(a) Consumer protection cooperation (CPC)

The EU has established two parallel systems for cross-border consumer protection cooperation. The first system is based on the Regulation on consumer protection cooperation (CPC Regulation) and governs both proactive (e.g. sweeps) and reactive (e.g. redress) cooperation among public authorities in the Member States as well as the European Commission in fulfilling the goals of consumer protection.

The second system – i.e. the European Consumer Centres Network (ECC-Net) – constitutes a network of (predominantly) non-governmental bodies tasked with proactive (e.g. advise) and reactive measures (e.g. assistance in redress mechanisms) towards the common goal of consumer protection [cf. Sect. 2.3.20].

\(^{82}\) OJ L 84, 20.03.2014, pp. 42–56.
\(^{83}\) OJ L 165, 18.06.2013, pp. 1–12.
\(^{84}\) OJ L 165, 18.06.2013, pp. 63–79.
\(^{85}\) OJ L 171, 02.07.2015, pp. 1–4.
1. Introduction

The enforcement of EU legislation concerning consumers’ economic interests was strengthened in 2004 with the adoption of the Consumer Protection Cooperation Regulation (CPC Regulation). This unique framework brings together national authorities from all EU Member States. Its primary aim is to tackle cross-border infringements by establishing procedures for information exchange, cross-border enforcement requests and coordinated actions, to prevent infringing traders from moving between Member States to exploit gaps in jurisdictional boundaries. It also permits the conclusion of international cooperation agreements. […]

The review process thus far confirmed that the implementation of the CPC Regulation in 2007 led to the development of effective means to safeguard consumers’ collective interests across the EU. The CPC Regulation set common minimum enforcement capacities for national authorities and allowed them to conduct joint enforcement actions coordinated by the European Commission. For example, more than 3,000 ecommerce websites in various economic sectors were screened for infringements of EU law resulting in increased compliance. In the last two years, a further step was made to require the industry to cease unfair commercial practices in areas of common interest across the EU – common CPC enforcement approaches. A recent CPC action on in-app purchases, which saw national enforcement authorities across the EU present large technology companies with a common understanding of how to apply relevant consumer rules in this area, is a concrete example of how CPC-led enforcement can deal with modern consumer problems occurring in a number of Member States. […]

2. Since 2007, enforcement cooperation has increased the benefits of EU consumer legislation for consumers

Since 2007, the CPC Regulation has brought substantial benefits to EU consumers thanks to the strengthening of enforcement capacities throughout Europe. Cooperation among consumer protection enforcement authorities has ensured a more uniform application of EU consumer protection laws, contributing to the better functioning of the Single Market for citizens and businesses. In particular:

- The CPC mutual assistance mechanism provided a clear and comprehensive legal framework for mutual exchanges of information and cross-border enforcement actions. The most important innovation is the possibility to enforce consumer protection law across borders (Article 8 of the CPC Regulation). This not only reduces the cost of enforcement but also permits the use of the administrative means of one country to the benefit of consumers from other countries and to prevent infringing traders from moving around. […]
- The “sweeps” and common enforcement approaches based on Article 9 of the CPC Regulation allowed the Member States to coordinate their enforcement approaches on a larger scale. They provided effective EU-wide tools for the detection and combating of serious and widespread infringements, with a clear deterrent effect on other traders. Corrective measures taken, for instance, in the areas of electronic goods, travel services and digital content clearly led to a measurable increase of compliance and awareness about consumer rights among businesses. […]
- The CPC alert mechanism provided for the first time a framework for Member States to exchange information about emerging infringements and to determine infringements which may require a coordinated approach.
- Common activities and projects, workshops and other events boosted the enforcement and administrative capacity of the Member States in consumer protection and led to an increase in trust and mutual understanding among Member States’ authorities involved in the CPC network.
- International cooperation allowed the exchange good practices with the EU’s main trading partners. […]

6. Clarification of the main components of the CPC Regulation

The CPC network

The CPC Regulation requires the Member States to designate public enforcement authorities (“competent authorities”) in charge of enforcement of the EU consumer laws listed in the Annex to the CPC Regulation as well a single liaison office, responsible for coordinating CPC matters in each Member State. They form the CPC network. Member States must ensure that adequate resources are allocated to these authorities to perform
Consumer protection cooperation

their CPC duties.

The network of competent authorities was considerably extended over the period 2007-2013. The main reason for this was the gradual extension of the material scope of the CPC Regulation, as new EU legislation was added to its Annex. […]

Diversity of national enforcement systems and barriers to cooperation

The CPC Regulation acknowledges the role that judicial authorities may play in national enforcement systems: the competent authorities may exercise their powers either under their own authority or under the supervision of the judicial authorities or by application to courts. There is great variation across Member States as regards the judicial authorities' involvement in public enforcement proceedings. […]

A large majority of stakeholders in the public consultation agreed that the introduction of common standards to handle CPC-relevant infringements would be useful and thought that defining such standards would be a high priority in the areas of enforcement decisions' publication, naming of infringing traders, access to documents, evidence gathering and websites investigation. […]

Involvement of consumer organisations and other actors in CPC cooperation

The CPC Regulation acknowledges the consumer organisations' essential role in the protection of consumer interests. It enables, in particular, Member States to designate, besides public authorities, other bodies having a legitimate interest to stop intra-Union infringements. These bodies can be instructed by the CPC authorities to take necessary enforcement measures available to them under national law to stop intra-Union infringements.

In the period 2007-2013, several Member States have designated such bodies. They mostly comprise consumer associations and group interest associations acting in their own name. Also, since several years, national consumer organisations co-operate closer and coordinate enforcement activities under the Consumer Justice Enforcement Forum (COJEF) project. Many Member States developed cooperation with consumer associations and European Consumer Centres to obtain information about market developments and infringements. […]

The CPC database

The CPC Regulation (Article 10) mandates the Commission to maintain an electronic database where the information related to mutual assistance requests and alerts is stored and processed. To this effect, the Commission put in place the CPC-System (CPCS). Since 2007, the CPCS has been improved to allow the CPC authorities to exchange information and documents pertaining to mutual assistance requests. The Biennial reports, the Evaluation and the public consultation results indicate dissatisfaction with the CPCS. They point out that the lack of a well-functioning IT tool is a barrier to effective CPC cooperation.

7. Strengthening of CPC common and international activities

[…] International cooperation of enforcement of consumer rights

Developments in technology and household consumption patterns towards a greater use of international online purchasing have reinforced the need to deter dishonest traders from third countries and to enforce consumer protection beyond the EEA.

The CPC Regulation provides that the Union “shall cooperate with third countries and with the competent international organisations in the areas covered by this Regulation in order to enhance the protection of consumers’ economic interests”. Furthermore the Union has the possibility of seeking more structured enforcement cooperation with third countries on the basis of international agreements.

The competent authorities in the CPC network further cooperate on a regular basis in the ICPEN\(^\text{88}\) and the OECD or on a bilateral basis with third countries identified as priority partners for enforcement cooperation, such as the USA. This cooperation is a very important aspect of consumer policy and could be particularly useful for example in the field of data protection.


1.2 The Object of the Evaluation: The European Consumer Centres Network

The ECC-Net is a pan-European network which was established with the overall aim of promoting consumer confidence in the internal market. It consists of 29 centres located in 27 EU Member States plus Iceland and Norway. These centres deal only with business-to-consumer (B2C) issues, delivering a range of services to consumers such as: advising them on their rights when shopping cross-border (within the territories of the EU, Iceland and Norway); supporting and assisting consumers with their complaints; and, providing consumers with information and access to an appropriate Alternative Dispute Resolution (ADR) scheme in the event of a dispute.

The Network was created in 2005 by merging two previously existing networks:

- The European Consumer Centres or ‘Euroguichets’, which provided information and assistance to consumers on cross-border issues; and,
- The European Extra-Judicial Network (EEJ-Net) which helped consumers to resolve their disputes through ADR schemes using mediators or arbitrators.

There is no specific legal basis establishing the Network; it is foreseen as part of action 10.2 of European Parliament and Council Decision 1926/2006/EC establishing a programme for Community action in the field of Consumer Policy (2007-2013):

**Action 10.2:** Financial contributions for joint actions with public or non-profit bodies constituting Community networks which provide information and assistance to consumers to help them exercise their rights and obtain access to appropriate dispute resolution (the European Consumer Centres Network).

In the absence of a legal basis, the activities of the Network are governed by a ‘vademecum’ which specifies six categories of tasks (or operational objectives) for the ECCs:

1. **Promotional activities (Proactive):** to raise awareness of the Network and consumer rights by organising communication campaigns, seminars, workshops and conferences etc.; and, to cooperate with other EU-networks (e.g. SOLVIT FIN-NET);
2. **Provision of information (Reactive):** to respond to specific consumer enquiries about their rights when shopping across borders;
3. **Assistance with complaints:** to give advice and support to any consumer with a complaint related to a cross-border purchase;
4. **Assistance with disputes:** to provide easy access to ADR-bodies in situations where it has not been possible to resolve a cross-border consumer complaint amicably and to assist in this process;
5. **ADR development:** to collect information on national ADR schemes; and to assist the national authorities in the promotion and development of new out-of-court schemes; and,
6. **Networking and feedback:** to share information, problems and best practices with other centres in the Network; and to contribute to national and EU policy making processes.

The overall responsibility for the management of the ECC-Net lies with DG SANCO. However, certain parts of the management of the ECC-Net have recently been delegated to the Executive Agency for Health and Consumers (the Agency). Specifically, the Agency is responsible for financial management of the ECC-Net which inter alia includes the following functions: preparation and publication of calls for proposals; evaluation of proposals in conjunction with DG SANCO; award of grants and preparation of grant agreements; monitoring the implementation of grant agreements; assessment of the performance of the individual centres; ex post publicity; and, implementation of financial controls.

The Network is co-financed by the European Commission, the EU Member States, Norway and Iceland. The ECC host organisations are awarded grants on the basis of an annual call for proposals launched by the Agency.
Each year, the EU Member States and EFTA/EEA countries are invited to participate in the call for proposals, as part of which they also have to designate a host organisation for the ECC in their respective countries. The host organisations must also be a public body or a non-profitmaking body designated by the Member State (or by a competent authority in Iceland and Norway) and agreed by the European Commission.

(c) Online dispute resolution

One of the key components of the EU consumer protection policy is to increase the use of out-of-court methods for solving consumer disputes.

Online dispute resolution (ODR) constitutes an implementation of existing forms of alternative dispute resolution (ADR) enabled by information and communication technologies (ICTs). While various forms exist, negotiation, mediation and arbitration are the most widely practised ones, both in the business-to-consumer (B2C) and business-to-business (B2B) contexts (Savin 2013). The main assumption of alternative methods of dispute resolution – that is the out-of-court settlement in the presence of a neutral third party during the process of reaching an agreement – remains unchanged. However, ODR has attained a different character because of the use of modern forms of communication. The term covers disputes that are partially or fully settled over the Internet, having been initiated in cyberspace, both with a source inside (on-line) or outside it (offline). In the literature, the terms electronic ADR (eADR), online ADR (oADR) and Internet dispute resolution (iDR) are treated as synonymous. The number of electronic forms of alternative methods for dispute resolution changes over time, but mediation (74% of ODR providers) and arbitration (40% of ODR providers) are most frequently used (Mania 2015).

The main benefit of ADR mechanisms, including ODR, lies in their low-cost, rapid and easy nature, as compared to the use of ‘traditional’ courts of law, thus making them attractive for low value disputes, to which many consumer disputes belong to (cf. Clifford and Van Der Sype 2015). Further advantages lie in the exclusion of the problematic aspect of the choice of law [cf. Sect. 2.2.2(a)], as – put simply – in most cases the choice of law has been already made. However, their main drawbacks concern their voluntary nature and not always binding – thus un-enforceable – outcome; the latter simply depends on the ADR venue and ADR procedures chosen.

The use of ICTs for alternative dispute resolution is not a novelty per se. Perhaps the most known example is the Uniform Domain-Name Dispute-Resolution Policy (UDRP), supplemented by the Rules for Uniform Domain Name Dispute Resolution Policy, both developed by the Internet Corporation For Assigned Names and Numbers (ICANN) in 1999 and most recently amended in 2010.93 The UDRP is applicable in relation to entities that had unlawfully registered an Internet domain, endangering or infringing the rights to protection of trademarks of third parties. The UDRP sets the rules for concluding agreements on registration and administration of domains, including regulations that oblige disputes to be settled amicably and thus avoid problems involving the jurisdiction of courts (Mania 2015).

Since 2006, it is the Czech Arbitration Court (i.e. an arbitration court attached to the Czech Chamber of Commerce and Agricultural Chamber of the Czech Republic) that has been operating as the dispute resolution provider for the .eu domain name, itself launched in 2004.94 Disputes submitted to this Court are dealt with in accordance with the .eu Alternative Dispute Resolution Rules (.eu ADR).95

Conversely, less known is the mere fact that the recently fallen Safe Harbour Agreement contained a requirement to settle disputes by means of ADR.

Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU (2013)97

6. STRENGTHENING THE SAFE HARBOUR PRIVACY PRINCIPLES

6.1. Alternative Dispute Resolutions

96 CJEU, Maximilian Schrems v Data Protection Commissioner, 6 October 2015, case C-362/14.
The enforcement principle requires that there must be “readily available and affordable recourse mechanisms by which each individual’s complaints and disputes are investigated”. To that end the Safe Harbour scheme establishes a system of Alternative Dispute Resolution (ADR) by an independent third party to provide individuals with rapid solutions. The three top recourse mechanisms bodies are the EU Data Protection Panel, BBB (Better Business Bureaus) and TRUSTe.

The use of ADR has increased since 2004 and the Department of Commerce has strengthened the monitoring of American ADR providers to make sure that the information they offer about the complaint procedure is clear, accessible and understandable. However, the effectiveness of this system is yet to be proven due to the limited number of cases dealt with so far.

Though the Department of Commerce has been successful in reducing the fees charged by the ADRs, two out of seven major ADR providers continue to charge fees from individuals who file a complaint. This represents the ADR providers used by about 20% of Safe Harbour companies. These companies have selected an ADR provider that charges a fee to consumers for filing a complaint. Such practices do not comply with the Enforcement Principle of Safe Harbour which gives individuals the right of access to a “readily available and affordable independent recourse mechanisms”. In the European Union, access to an independent dispute resolution service provided by the EU Data Protection Panel is free for all data subjects.

On 12 November 2013 the Department of Commerce confirmed that it “will continue to advocate on behalf of EU citizens’ privacy and work with ADR providers to determine whether their fees can be lowered further”. […]

In order to give full effect to the EU consumer policy, comprising the fundamental right to consumer protection (cf. Art 38 EU CFR; Art 169 TFEU), the EU embarked on a project to increase the use of ADR mechanisms in consumer disputes, in particular by developing a platform for on-line dispute resolution (ORD) of such disputes. To that end, a Directive on Consumer ADR – promoting the use of ADR in general – and a Regulation on Consumer ODR – establishing the said platform – have been enacted in 2013. The ODR Regulation is interconnected with the Directive on consumer ADR in a sense that the ODR Regulation constitutes a complement to the ADR Directive and must be read in conjunction therewith (Bogdan 2015, 156). The platform became fully operational on 15 February 2016.98

### Directive on Consumer ADR (2013)

**Article 5**
**Access to ADR entities and ADR procedures**

1. Member States shall facilitate access by consumers to ADR procedures and shall ensure that disputes covered by this Directive and which involve a trader established on their respective territories can be submitted to an ADR entity which complies with the requirements set out in this Directive.

### Regulation on Consumer ADR (2013)

**Article 1**
**Subject matter**

The purpose of this Regulation is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market, and in particular of its digital dimension by providing a European ODR platform (‘ODR platform’) facilitating the independent, impartial, transparent, effective, fast and fair out-of-court resolution of disputes between consumers and traders online.

**Article 2**
**Scope**

1. This Regulation shall apply to the out-of-court resolution of disputes concerning contractual obligations stemming from online sales or service contracts between a consumer resident in the Union and a trader established in the Union through the intervention of an ADR entity listed in accordance with Article 20(2) of

Directive 2013/11/EU and which involves the use of the ODR platform.

2. This Regulation shall apply to the out-of-court resolution of disputes referred to in paragraph 1, which are initiated by a trader against a consumer, in so far as the legislation of the Member State where the consumer is habitually resident allows for such disputes to be resolved through the intervention of an ADR entity. […]

Article 5
Establishment of the ODR platform

1. The Commission shall develop the ODR platform (and be responsible for its operation, including all the translation functions necessary for the purpose of this Regulation, its maintenance, funding and data security. The ODR platform shall be user-friendly. The development, operation and maintenance of the ODR platform shall ensure that the privacy of its users is respected from the design stage (‘privacy by design’) and that the ODR platform is accessible and usable by all, including vulnerable users (‘design for all’), as far as possible.

2. The ODR platform shall be a single point of entry for consumers and traders seeking the out-of-court resolution of disputes covered by this Regulation. It shall be an interactive website which can be accessed electronically and free of charge in all the official languages of the institutions of the Union.

3. The Commission shall make the ODR platform accessible, as appropriate, through its websites which provide information to citizens and businesses in the Union and, in particular, through the ‘Your Europe portal’ established in accordance with Decision 2004/387/EC.

4. The ODR platform shall have the following functions:

(a) to provide an electronic complaint form which can be filled in by the complainant party in accordance with Article 8;
(b) to inform the respondent party about the complaint;
(c) to identify the competent ADR entity or entities and transmit the complaint to the ADR entity, which the parties have agreed to use, in accordance with Article 9;
(d) to offer an electronic case management tool free of charge, which enables the parties and the ADR entity to conduct the dispute resolution procedure online through the ODR platform;
(e) to provide the parties and ADR entity with the translation of information which is necessary for the resolution of the dispute and is exchanged through the ODR platform;
(f) to provide an electronic form by means of which ADR entities shall transmit the information referred to in point (c) of Article 10;
(g) to provide a feedback system which allows the parties to express their views on the functioning of the ODR platform and on the ADR entity which has handled their dispute;
(h) to make publicly available the following:
   (i) general information on ADR as a means of out-of-court dispute resolution;
   (ii) information on ADR entities listed in accordance with Article 20(2) of Directive 2013/11/EU which are competent to deal with disputes covered by this Regulation;
   (iii) an online guide about how to submit complaints through the ODR platform;
   (iv) information, including contact details, on ODR contact points designated by the Member States in accordance with Article 7(1) of this Regulation;
   (v) statistical data on the outcome of the disputes which were transmitted to ADR entities through the ODR platform.

5. The Commission shall ensure that the information referred to in point (h) of paragraph 4 is accurate, up to date and provided in a clear, understandable and easily accessible way.

6. ADR entities listed in accordance with Article 20(2) of Directive 2013/11/EU which are competent to deal with disputes covered by this Regulation shall be registered electronically with the ODR platform.

7. The Commission shall adopt measures concerning the modalities for the exercise of the functions provided for in paragraph 4 of this Article through implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 16(3) of this Regulation.
Observations

(a) Multilingualism

Regulation on consumer protection cooperation (2004)

Article 12
Request for mutual assistance and information exchange procedures

[…]
4. The languages used for requests and for the communication of information shall be agreed by the competent authorities in question before requests have been made. If no agreement can be reached, requests shall be communicated in the official language(s) of the Member State of the applicant authority and responses in the official language(s) of the Member State of the requested authority.

Regulation on Consumer ADR (2013)

Article 5
Establishment of the ODR platform

[…]
2. The ODR platform shall be a single point of entry for consumers and traders seeking the out-of-court resolution of disputes covered by this Regulation. It shall be an interactive website which can be accessed electronically and free of charge in all the official languages of the institutions of the Union.

The problem of multiple languages in the cross-border consumer protection cooperation has been solved – again – at the supranational level, using two methods: while the competent authorities need to agree beforehand on the language of communication between them, the consumer always has a possibility to communicate to these authorities in her own language.

(b) Use of technology

The mechanisms for consumer protection cooperation, in particular in the area of enforcement of consumer rights, heavily depend on sharing relevant information and this occurs with the help of technology. Both systems – i.e. CPC Regulation and ECC-Net – use devoted databases to share case-related information. Already operational for a couple of years, these databases have been scrutinized by external evaluators. We have found the results thereof extremely useful when it comes to their practical functioning.

Regulation on consumer protection cooperation (2004)

Article 10
Database

1. The Commission shall maintain an electronic database in which it shall store and process the information it receives under Articles 7, 8 and 9. The database shall be made available for consultation only by the competent authorities. […]

2. Where a competent authority establishes that a notification of an intra-Community infringement made by it pursuant to Article 7 has subsequently proved to be unfounded, it shall withdraw the notification and the Commission shall without delay remove the information from the database. Where a requested authority notifies the Commission under Article 8(6) that an intra-Community infringement has ceased, the stored data relating to the intra-Community infringement shall be deleted five years after the notification.

99 These concern: exchange of information without request (Art 7), requests for enforcement measures (Art 8) and coordination of market surveillance and enforcement activities (Art 9) [footnote ours].
5.7 Data management issues

The efficiency of the CPCS is dependent on the efficiency of the processes set up to enable Member State authorities to deal with information and enforcement requests and alerts. There is the perception that the CPCS process is slow and complex and that this limits the effectiveness of the system. A number of issues were highlighted on the functioning of the system in case studies and in-depth interviews:

- The data forms required to be filled in were felt to be excessively lengthy and time consuming. In one instance, an SLO specified that the data required to be entered into the system was sufficiently complicated that a preliminary file was prepared in Microsoft Word format to facilitate the process of data entry. (“Entering info in the CPC Web page is very complicated and usually before entering information [our] staff prepare it in a Word document.”)
- The CPC servers are often extremely slow (this was highlighted by interviewees in four out of the nine countries where detailed interviews were undertaken) and liable to frequent crashes.
- A specialist from one NCA mentioned that the storage capacity of the CPC system is low in that attachments exceeding a size of 2MB cannot be transferred. This resulted in difficulties in attaching and sending evidence of infringements, particularly in instances where infringing websites had been photographed and the evidencing attachment was required to be sent to other Member States (given the obligation of the Regulation for evidence of infringement to be provided wherever possible).
- The system is not user-friendly and it is difficult to gain a comprehensible overview of information obtained, even in PDF format. One recommendation relating to increasing user-friendliness concerned bringing the ‘TESTA’ tool in line with alternative secured Internet addresses: “According to the national competent authorities’ feedback, the TESTA IT-tool is not user-friendly and therefore not very operational. Some national authorities are not yet connected to the CPC Network, because the system obliges dedicated lines and a specific contract with a telecommunications provider involving secured lines and additional features that imply high costs for those authorities. In the future, maybe the TESTA IT-tool could be further developed under the same model of other secured Internet addresses (normal https:// addresses like the ones used by banks) that could work in a less costly and friendly way.” [SLO]
- Files provided through the system do not always bear an official seal of approval (from the Commission), which often renders them unusable in a court of law. (“There is still a lot to do in terms of improving the quality of documents/data available for court proceedings – for instance, we have often had difficulties in proving an infringing trader wrong in court simply because of a lack of authentication of documents provided by requested MS. At the moment we are only able to use “print-screen” documents of the information provided which unfortunately do not contain the Commission’s official seal – authenticity of documents is therefore very much questioned in court proceedings. The Commission should review how best to present data information.”)

Stakeholders consulted indicated that a range of alternatives were in place at the national level in selected Member States that were helpful overcome the shortcomings of the CPCS. These could potentially serve as models for Member States which do not have parallel setups in place. In addition to the CPCS, information stored on centralised national databases is often referred to in order to double-check against available data on infringing traders. Examples of such databases are as follows:

- The “Baromètre des réclamations” (FR);
- Central Database to monitor complaints and reports (BE);
- ‘Consumer regulation’ website (UK);
- Internal databases (EE, not publicly accessible).

In one instance, a national database was specified to have been tailored such that professional sectors where the likelihood of infringements occurring was higher were rapidly identified to encourage more effective enforcement actions. Another NCA stated that an alternative website was employed for transferring data files exceeding 2MB in size. The CIRCA platform was mentioned as a potential alternative to CPCS in some circumstances (e.g. for scheduling meetings).

Recommendations made by those consulted to increase the effectiveness of CPCS processes included:

- Increased user-friendliness of processes by means of shorter data entry forms, increased storage capacity,

---

simplified information display formats and reduced access restrictions for authorised national agencies;
- Ensuring the provision of more rapid and better targeted search results;
- Potential for a greater role played by the European Commission in ensuring that information available on CPCS is up to date and in setting up automated reminders for timely responses to data requests;
- Ensuring that all documents stored on the system have an official CPC seal of authentication (and can therefore be presented in a court of law), as there is currently no provision for the Commission to certify that appropriate documentation or evidence has been attached to CPC forms even as the format of print-outs of these forms has been improved;
- Establishment of a communication infrastructure between Member State authorities and provision of contact details of NEBs\(^\text{101}\) in other Member States; and
- Enhanced ease of access to information on case laws and upcoming cases. In its latest biennial progress report, the Commission indicated that measures have been initiated to address several of the issues highlighted above. In particular, new IT functionalities are due to be launched in 2012 to better coordinate enforcement activity and to allow for more effective searches. Further, the tool is in the process of being made multilingual and operational speeds are likely to increase in the near future. The nature of data protection under the system, while fairly satisfactory, is being further refined in consultation with the European Data Protection Supervisor (EDPS).

**Period of enforcement data retention on the common database**

Under the provisions of the CPC Regulation, enforcement data is to be retained in the common CPC database for a period of 5 years. The purpose of this provision is to facilitate effective enforcement of the Regulation by ensuring that Member State authorities are able to track infringements and, in particular, traders who persistently violate consumer law provisions.

In the in-depth interviews undertaken as part of the study, stakeholders were asked to comment on whether this data retention period was adequate in terms of promoting effective enforcement. All the authorities interviewed expressed satisfaction that 5 years was an appropriate duration for data retention, in particular given that this duration is calculated beginning from the closing date of each case, as was specified by one SLO. In addition, an SLO interviewee suggested that while retention for 5 years was crucial, further retention might provide additional benefits in cases of recidivism over periods exceeding 5 years. Another SLO emphasised the significance of deleting data on traders who had fully complied with the law after having been identified and named in the database after 5 years, as not doing so would result in ‘reformed’ traders being unfairly penalised. One other SLO suggested that while 5 years served as an adequate retention period on the whole, a separate database could be envisaged to focus on the most commonly occurring types of infringement, data on which could potentially be retained for a longer period.

---

\(^{101}\) National enforcement body [footnote ours].


**Article 14**

**Case handling database**

1. The Commission shall maintain an electronic database in which the cases handled by the ECC-Net must be introduced. Where appropriate, complaints should be introduced via the pdf/online complaint form. The details of a complaint shall be introduced in the database in accordance with guidelines provided by the European Commission and as indicated in the case handling protocol;
2. The ECC-Net shall provide to each other mutual and reciprocal assistance regarding the cases introduced in the database. Cases shall be introduced by the ECC where the consumer is resident and dealt with by the ECC of the country where the trader is located.
3. The ECC-Net shall develop experience in handling the cases by sharing such experience within the Network during its activities such as meetings, joint projects, etc.
3.2.11 Q.17 Are the processes and procedures in place (Case Handling IT tool, other tools, human resources, workflows and organisational solutions) in line with the objectives?

[...] Lack of protocols for sharing cases with other organisations

Another issue highlighted by the case studies is that a number of ECCs have not put in place formal protocols for signposting or sharing of cases with other national stakeholders such as enforcement bodies, ADRs, consumer organisations etc. There are some exceptions. For example, ECC-Belgium has signed a protocol with DG Enforcement and Mediation which determines the cooperation between the two organisations on matters such as exchange of information and mutual assistance. Some ECCs (e.g. Luxembourg, Malta) have formal protocols for case sharing with NEBs.

Although where cooperation is informal, the ECCs and stakeholders generally think that it ‘works well’ and most ECCs are of the view that there is no need for formalisation of transfer/sharing of complaints. However, it was noticed that this way of working has certain disadvantages, e.g. the NEB does not seem to be aware of the role and functions of the ECC in Slovenia, despite ECC promotional material being regularly sent to the NEB, according to the ECC Director. Moreover, much of the evaluation evidence suggests that structured cooperation between the ECCs and enforcement bodies (including the NEBs) would benefit consumers. [...] [T]he ECCs and enforcement bodies could establish a formal protocol for handling cases relating to individual infringements of a given piece of EU legislation and/or notification of traders who systematically breach EU consumer legislation. [...]
(c) Costs

While the cost of cooperation within the CPC Regulation is borne by each Member State individually, it is the general budget of the EU that funds the ECC-Net.

<table>
<thead>
<tr>
<th>Regulation on consumer protection cooperation (2004)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 15 Conditions</td>
</tr>
<tr>
<td>1. Member States shall waive all claims for the reimbursement of expenses incurred in applying this Regulation. However, the Member State of the applicant authority shall remain liable to the Member State of the requested authority for any costs and any losses incurred as a result of measures held to be unfounded by a court as far as the substance of the intra-Community infringement is concerned. [...]</td>
</tr>
</tbody>
</table>

(d) Gradual development

<table>
<thead>
<tr>
<th>Regulation on consumer protection cooperation (2004, as amended 2011)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 21a Review</td>
</tr>
<tr>
<td>By 31 December 2014, the Commission shall submit a report to the European Parliament and to the Council which shall assess the effectiveness and operational mechanisms of this Regulation and thoroughly examine the possible inclusion in the Annex of additional laws that protect consumers’ interests. The report shall be based on an external evaluation and extended consultation of all relevant stakeholders, and shall be accompanied, where appropriate, by a legislative proposal.</td>
</tr>
</tbody>
</table>

(e) Coordinated enforcement activities (‘sweeps’)

<table>
<thead>
<tr>
<th>Regulation on consumer protection cooperation (2004)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 9 Coordination of market surveillance and enforcement activities</td>
</tr>
<tr>
<td>1. Competent authorities shall coordinate their market surveillance and enforcement activities. They shall exchange all information necessary to achieve this.</td>
</tr>
<tr>
<td>2. When competent authorities become aware that an intra-Community infringement harms the interests of consumers in more than two Member States, the competent authorities concerned shall coordinate their enforcement actions and requests for mutual assistance via the single liaison office. In particular they shall seek to conduct simultaneous investigations and enforcement measures.</td>
</tr>
<tr>
<td>3. The competent authorities shall inform the Commission in advance of this coordination and may invite the officials and other accompanying persons authorised by the Commission to participate. [...]</td>
</tr>
</tbody>
</table>


5.8 SWEEPS

Since 2007 the Member States have organised concerted actions called ‘SWEEPS’, under Article 9 of the CPC Regulation which calls on competent authorities to coordinate their market surveillance and enforcement activities when the interests of consumers in more than two Member States are potentially harmed by an infringement. SWEEPS are a means to foster a common approach and enhance enforcement in the EU. Together with alerts, information requests and enforcement requests, common surveillance activities constitute one of the coordination mechanisms of the CPC Network. SWEEPS are amongst the most visible of these activities. Participation in a SWEEP is undertaken on a voluntary basis.
The objective of SWEEPS is to investigate whether online businesses comply with EU and national consumer protection laws, and to improve the compliance with such laws across the EU. Coordination on a simultaneous basis and seeking enforcement along the same lines should improve the effectiveness of the action and contribute to a new “European dimension” to enforcement. Such EU wide actions have a clear facilitation effect on the single market and because SWEEPS fight non-compliant online traders at both national and cross-border level, there is often a strong domestic benefit from being involved. In exchanging information to achieve coordination there is also added benefits in terms of the opportunity for authorities in the same area to establish contacts, share experience and discuss best practices and develop a common understanding of legal issues.

In each SWEEP action, national authorities check hundreds of sites relating to a particular sector or product in order to check whether the necessary consumer rights are being adhered to. The sectors proposed for the SWEEP are selected by Member States with the Commission based on a list of proposed themes that combines evidence on current consumer issues available to national authorities and the Commission (e.g. data from the ECC-Net database).

A SWEEP action comprises two steps. In the first phase the initial checks are undertaken where national authorities decide whether a particular website should be recommended for further investigation. The websites are checked against a checklist agreed on by the participating NCAs before the SWEEP, and is used by all participating Member States. In the second phase the authorities investigate suspected websites further and take appropriate follow-up actions, if necessary through the CPC Network. They contact the traders responsible for the websites under investigation asking for clarification and correction of the irregularities.

So far SWEEPS have been carried out in the following areas: websites selling air tickets (2007); mobile phone contents (2008); electronic goods (2009); tickets for cultural and sports events (2010); and, consumer credits providers (2011). […] The nature of SWEEPS ensures a strong cross-border dimension; a SWEEP is also highly beneficial at national level. As one stakeholder described it:

‘[…] it is difficult to find a legal basis that would give […] the power to do an Internet Sweep. But thanks to the Commission, […] was able to do this and detect infringements.’

In addition, the evidence from the SWEEP actions suggests that the number of national websites subject to investigation greatly exceeded cross-border cases. […] This reflects different characteristics of consumer credit and airline markets, the former being highly domestic and the latter highly cross-border.

The cross-border dimension does not prevent authorities focussing on national cases, as when dealing with other enforcement issues described earlier. Indeed, the EC noted that in the Airline SWEEP, Finland did not follow five cross border cases because they ‘decided to concentrate their effort in correcting national cases’. If this was the case, it is important that the reasons behind authorities’ behaviour are understood. Indeed, stakeholders’ interviews showed that there are resource issues with regards to SWEEPS with the majority expressing the need for improvements in cross-border cooperation. […]

Investigating the SWEEP data further, the figures show that in the airline SWEEP only 12% of total reported cross-border cases were corrected through enforcement action compared with 56% of national cases. If the same is the case for other SWEEPs (for which data are not available), this suggests that there is significant scope for improvement in cross-border enforcement. Also SWEEP results indicate high infringement levels in national contexts. SWEEP action helps to identify and trigger follow-up to such domestic cases and thus raises the overall level of consumer protection. […]

Further ‘sweeps’ have been conducted for digital contents (2012) and travel services (2013).102 It is fair to say that annual sweeps have become the key feature of the CPC Regulation. They all prove the fact that coordinated pan-EU ex ante investigations and enforcement activities have the potential to lead to positive results for consumers. In each case, compliance with EU laws had massively improved (Wrbka 2014).

In the area of data privacy law, the Global Privacy Enforcement Network (GPEN)103 launched such ‘sweeps’ already in 2013 and by now the initiative has reached considerable success. The first one was devoted to the notion of transparency104 and most recent one (2015) dealt with protection of children online.

---

GATINEAU, Quebec, September 2, 2015 – The third Global Privacy Enforcement Network (GPEN) Privacy Sweep demonstrates the ongoing commitment of privacy enforcement authorities to work together to promote privacy protection around the world.

Twenty-nine privacy enforcement authorities in 21 countries participated in this year’s Sweep, which took place May 11-15, 2015. That’s up from 26 participating authorities last year. Over the course of the week, participants visited 1,494 websites and mobile applications (apps) that were either targeted at or popular among children. The aim: to determine whether apps and websites are collecting personal information from children, what personal information is being collected, whether protective controls exist to effectively limit the collection and whether the information could be easily deleted. [...]

About the GPEN Privacy Sweep:

The goals of the Sweep initiative included: increasing public and business awareness of privacy rights and responsibilities; encouraging compliance with privacy legislation and enhancing cooperation among privacy enforcement authorities.

The Sweep was not an investigation, nor was it intended to conclusively identify compliance issues or possible violations of privacy legislation. The Sweep was also not an assessment of an app or website’s privacy practices in general, nor was it meant to provide an in-depth analysis of the design and development of the apps or websites examined.

By briefly interacting with the apps and websites, the exercise was meant to recreate the consumer experience. Our sweepers ultimately sought to assess privacy practices by spending a few minutes per website or app checking performance against a set of common indicators.

GPEN Privacy Sweep efforts are ongoing. As was the case in previous years, concerns identified during the Sweep could result in follow-up work such as outreach to organizations and/or enforcement action. The Office of the Privacy Commissioner of Canada has also prepared a classroom activity for Grade 7 and 8 teachers based on the Sweep to help familiarize students with privacy policies and issues related to the collection of personal information online.

The use of cross-border ‘sweeps’, both inside the EU as well as outside, should become an annual practice of data privacy authorities.

(f) Alternative Dispute Resolution (ADR)

Clifford and Van Der Sype (2015) have evaluated a possibility of employing the ADR Directive and the ODR platform to the disputes between data subjects, on the one hand, and data controllers and processors, on the other. They generally argue for suitability of such disputes to be solved by out-of-court procedures, predominantly due to their usually low value (in monetary terms), yet pointing out three problems that the current wording of the ADR Directive might pose for that type of disputes:

There has been some debate as to whether the EU consumer protection mechanisms are applicable to goods/services which do not demand payment but instead require the surrendering of personal data. Unsurprisingly, this uncertainty persists in relation to the enforcement mechanisms provided to EU consumers. Article 2 of the ADR Directive states that it applies to:

“procedures for the out-of-court resolution of domestic and cross-border disputes concerning contractual obligations stemming from sales contracts or service contracts between a trader established in the Union and a consumer resident in the Union through the intervention of an ADR entity which proposes or imposes a solution or brings the parties together with the aim of facilitating an amicable solution.”

This provision is repeated in the ODR Regulation. Hence, the dispute must follow from contractual obligations

stemming from sales or service contracts. In relation to the provision of services such as those provided by a social networking site, the scope debate is comprised of three key components. First, that such ‘free’ services must come within the definition of a service contract. Second, that the privacy and data protection requirements can be implied in a service contract without explicit reference and finally third, that the dispute must occur between a trader and a consumer both established in the EU. […]

The analysis in this article is based upon the assumption that the relationship between website owners and the user is seen as a service agreement, and the Terms and Conditions are deemed to be a service contract. Hence, although it is clear that these mechanisms will have applicability in relation to personal data disputes which arise from contracts that have monetary consideration (i.e. in the purchasing of applications on a mobile market), we can also assume the applicability of the EU ODR Regulation and ADR Directive in the context of disputes relating to personal data regarding goods and services offered as ‘free’. […]

The second component relates to the requirement that the dispute must stem from contractual obligations. It appears clear that this requirement is satisfied when a dispute arises from a breach of a Terms of Use in which privacy and data protection are mentioned explicitly. However, the situation is not clear when the terms do not explicitly provide guarantees for privacy and data protection. Hence, the question becomes whether privacy and data protection can be implied in the service contract thereby furthering the terms explicitly mentioned and implicitly recognising the data protection and privacy requirements. This is the case as compliance with the law is implied in any contractual arrangement and would thus be a statutory implied term within the terms of use. […]

[Third,] the application of this mechanism is thus limited to trader-consumer disputes. […] It is also significant to note that although reference is made to a ‘consumer’ this is not limited to an individual. […] Such a collective ADR mechanism could come within the operation of the ODR Regulation and could also provide a redress mechanism in relation to collective claims. Finally, it must also be noted that both the trader and the consumer must be established in the EU. […]

However, a viable supplement to the current system would be beneficial and the incorporation of ODR for data protection disputes could foster a new era of increased consumer awareness and empowerment.

We further add that both ADR Directive and the ODR platform should not be seen as the only possibility permitting the use of ADR mechanisms for solving data privacy disputes between data subjects and data controllers and processors. The proposal for the GDPR itself, in the wording as of December 2015, explicitly offers such a possibility to be introduced by means of codes of conduct (Art 38).


Article 38
Codes of conduct

[…] 1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes for the purpose of specifying the application of provisions of this Regulation, such as: […]

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

ADR mechanisms for solving data privacy disputes between data subjects and data controllers and processors, in particular in cross-border cases in the EU, should be encouraged both by policy makers and the supervisory authorities themselves. We acknowledge this would require further studies, in particular as to the role of the supervisory authorities, especially if they can act as a neutral party in such disputes.
2.4 Competition law cooperation

2.4.1 Legal framework

- 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\(^{106}\)
- Commission Notice on cooperation within the Network of Competition Authorities (2004)\(^{107}\)

2.4.2 General overview

**Dariusz Kloza and Anna Mościbroda, “Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law”, 4 International Data Privacy Law 2 (2014)\(^{108}\)**

**General remarks on the enforcement of the EU competition law**

Competition policy, together with, for example, a customs union and four freedoms, is one of the main building blocks of the internal market. It constitutes an exclusive competence of the EU, meaning that the EU alone is entitled to act and legislate in this field.

The EU competition rules were adopted so as to prevent the internal market being distorted by the private agreements partitioning it or by monopoly abuse. The main provisions on competition have been part of EU primary law since the Treaty of Rome (1957), providing for a single, directly applicable and directly effective legal framework in all Member States. In particular, Article 101 of the Treaty on the Functioning of the European Union (TFEU) deals with anticompetitive agreements, concerted practices, and decisions of association of undertakings, and Article 102 TFEU deals with abuses of a dominant position. Regulation 1/2003, a directly applicable instrument, supplements the Treaty with provisions defining the decision-making powers of the Commission and of the National Competition Authorities (NCAs) (if acting as enforcers of EU law) along with a core of procedural rules applied by the Commission, including its investigatory powers.

EU law is typically enforced in a decentralized manner. The obligation to enforce rests predominantly on national enforcement agencies and national courts. For many years, in the domain of EU competition law, it was the European Commission that—for the sake of ensuring coherence and avoiding potentially different interpretations of (then) European Community competition law at a national level—was given the role of a central enforcement authority. In particular, the Commission had sole competence to grant exemption from the prohibition of anticompetitive agreements in cases where the conditions for such exemption were fulfilled [Art. 101(3) TFEU]. All undertakings wishing to benefit from the exemption were obliged to notify their agreements to the Commission.

In 2004 Regulation 1/2003 entered into force and modernized the enforcement of EU competition law, marking a transition to a more decentralized enforcement. As a result, both the Commission and NCAs are equally empowered and obliged to apply Articles 101–102 TFEU in full. Those provisions can also be invoked in national courts. The Commission, however, remains at the heart of the competition law enforcement system.

The Treaty provisions on competition, that is, Articles 101–102 TFEU, apply to cases where an alleged infringement affects trade between the Member States; national competition law regulates purely domestic cases. An NCA, when it applies EU law to a case, may also apply in parallel its national rules to the same case. Therefore, EU competition law does not suppress but coexists with national provisions on competition. Hence, there is the possibility of a single case affecting more than one jurisdiction and thus being dealt with by more than one NCA as well as the possibility of a parallel application of EU and national laws. This has called for a set of rules regulating the relationship between EU and national laws, the allocation of cases, mechanisms to ensure consistency, and assistance in investigatory measures. Such rules constitute the building blocks of the ECN, which is discussed next.

**The functioning of the European Competition Network**

The European Competition Network (ECN) is a forum for the cooperation of European competition authorities in the application of EU competition law. Established in 2004 under Regulation 1/2003, the ECN consists of the Commission and of Member States’ NCAs. Given that both the Commission and NCAs are equally empowered and obliged to apply Articles 101–102 TFEU and given that a case might be of interest to more than one
agency, the need for efficiency required a mechanism for the allocation of cases between ECN members: hence rules were provided enabling the best-placed authority to deal with the case and discharging other authorities from the obligation to act. However, a parallel investigation by more than one NCA regarding the same conduct is not entirely precluded.

It was therefore necessary to ensure that NCAs avoid contradictory decisions and apply EU competition law in a consistent manner, ensuring the coherent development of EU competition law and policy. To this effect, Regulation 1/2003 provides for consistency mechanisms through an obligation imposed on participating authorities to consult any draft decision within the network. Regulation 1/2003 also confirms that Commission decisions take precedence over those of NCAs, as well as obliges NCAs to stay their proceedings should the Commission decide to act on the case.

Another objective of the ECN is an efficient division of work between participating NCAs and overall effective enforcement of EU competition law. Regulation 1/2003 allows for cooperation and assistance between the authorities as regards evidence-gathering and information exchange, in particular by:

- an exchange of information on the initiation of the investigations (obligatory);
- an exchange of information, including confidential information, which may be shared without the consent of the parties concerned; such information may be used as evidence (subject to some guarantees, eg limiting its use in criminal proceeding) (Art. 12);
- assistance in inspections: the Commission is obliged to inform an NCA of a planned inspection within its jurisdiction; similarly, an NCA is obliged to assist the Commission and the latter may request an NCA to carry out an inspection on its behalf [Art. 22(2)];
- an NCA may assist another NCA and undertake on its behalf fact-finding measures (eg inspections and interviews) [Art. 22(1)].

The ECN is an example of cooperation between NCAs based on a clear legal basis and allowing closer cooperation (including an exchange of confidential information) than traditional international instruments. For that reason, it became the reference point for cooperation in antitrust enforcement. Cooperation within the ECN applies only to the enforcement of EU competition law and is largely driven by the need to ensure the consistency of a unified framework. Still, ECN cooperation faces certain barriers, such as those connected with administrative burden (eg language issues and related costs). Also, remaining differences between Member States over leniency programmes or differences in levels of criminal liability for antitrust infringements may render the exchange of information more complex and subject to certain additional safeguards.


7. Regulation 1/2003 has considerably enhanced the enforcement of the EU competition rules by NCAs and national courts. NCAs and national courts not only have the power to apply the EU competition rules in full: they are obliged to do so when agreements or conduct are capable of affecting trade between Member States. These changes have considerably boosted enforcement of the EU competition rules by NCAs. The Regulation also introduced cooperation tools and obligations to ensure efficient work sharing and effective cooperation in the handling of cases and to foster coherent application. Building on these mechanisms, the ECN has developed into a multi-faceted forum for exchanges of experience on the application of substantive competition law as well as on convergence of procedures and sanctions. National courts play an essential role in the private enforcement of the EU competition rules. The Commission has sought to improve the effectiveness of private damages claims brought before national courts and a Directive on antitrust damages actions will be adopted soon.

8. There are now multiple enforcers of the EU competition rules, which has led to their much wider application. In the period covered from 1 May 2004 to 31 December 2013, the application of the EU competition rules has grown at a remarkable rate, with approximately 780 cases being investigated by the Commission (122) and the NCAs (665). Enforcement by the NCAs has developed in a broadly coherent manner.

2.4.3 Observations

(a) Firm legal basis

Dariusz Kloza and Anna Mościbroda, “Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law”, op. cit.

We observe that international cooperation in competition law enforcement develops particularly well within regional structures, that is among jurisdictions with similar cultural and legal backgrounds. A unified legal framework (eg as exists within the EU) justifies and enables close co-operation between enforcement authorities.

Cooperation within the ICN and the ECN demonstrate that both formal and informal cooperation mechanisms are crucial. The ICN is a valuable forum for informal cooperation and is regarded as particularly successful for trust building, sharing knowledge, and supporting capacity building, which is of particular importance for smaller and less experienced authorities. Being a forum for exchanging and preserving expertise and best practice amongst many, it also illustrates the particular usefulness and importance of multilateral cooperation. The ICN is also an example of structured cooperation, one which is focused on practical and case-handling issues. However, informal cooperation is unable to tackle problems underpinned by legal issues, for example legal obstacles to sharing confidential information. Recent studies of the OECD/ICN clearly indicate that a structured and legal response is required, ideally in the form of specific international law provisions on the matter. The ECN provides a unique example of tight and frequently used cooperation arrangement in competition law enforcement. Within the ECN, several cooperation mechanisms are explicitly regulated (eg exchange of confidential information or assistance in evidence gathering), which to large extent satisfy the requirements of efficient enforcement cooperation. […]

The lessons from the DPA cooperation case studies as well as examples of cooperation in the field of competition law teach us that efficient enforcement cooperation can take place only if there is a relevant framework fulfilling certain conditions. We have observed that such co-operation requires: (1) a firm legal basis, which implies its binding nature, and offers a structured and sufficiently detailed set of rules, which (2) define forms of cooperation, its conditions and procedures, including (3) provisions for the exchange of confidential or otherwise protected information (under appropriate conditions). We have also observed, as a prerequisite, that (4) such cooperation, in order to be effective, should have as broad a geographical scope as possible. These four elements constitute our building blocks of enforcement co-operation between DPAs.

Commission Notice on cooperation within the Network of Competition Authorities (2004)

2.2.3. Exchange and use of confidential information (Article 12 of the Council Regulation)

26. A key element of the functioning of the network is the power of all the competition authorities to exchange and use information (including documents, statements and digital information) which has been collected by them for the purpose of applying Article 81 or Article 82 of the Treaty. This power is a precondition for efficient and effective allocation and handling of cases.

27. Article 12 of the Council Regulation states that for the purpose of applying Articles 81 and 82 of the Treaty, the Commission and the competition authorities of the Member States shall have the power to provide one another with and use in evidence any matter of fact or of law, including confidential information. This means that exchanges of information may not only take place between an NCA and the Commission but also between and amongst NCAs. Article 12 of the Council Regulation takes precedence over any contrary law of a Member State. The question whether information was gathered in a legal manner by the transmitting authority is governed on the basis of the law applicable to this authority. When transmitting information the transmitting authority may inform the receiving authority whether the gathering of the information was contested or could still be contested. […]

2.2.4. Investigations (Article 22 of the Council Regulation)

29. The Council Regulation provides that an NCA may ask another NCA for assistance in order to collect information on its behalf. An NCA can ask another NCA to carry out fact-finding measures on its behalf. Article 12 of the Council Regulation empowers the assisting NCA to transmit the information it has collected to the requesting NCA. Any exchange between or amongst NCAs and use in evidence by the requesting NCA of such information shall be carried out in accordance with Article 12 of the Council Regulation. Where an NCA acts on behalf of another NCA, it acts pursuant to its own rules of procedure, and under its own powers of
3.1. Mechanism of cooperation (Article 11(4) and 11(5) of the Council Regulation)

43. The Council Regulation pursues the objective that Articles 81 and 82 of the Treaty are applied in a consistent manner throughout the Community. In this respect NCAs will respect the convergence rule contained in Article 3(2) of the Council Regulation. In line with Article 16(2) they cannot — when ruling on agreements, decisions and practices under Article 81 or Article 82 of the Treaty which are already the subject of a Commission decision — take decisions, which would run counter to the decisions adopted by the Commission. Within the network of competition authorities the Commission, as the guardian of the Treaty, has the ultimate but not the sole responsibility for developing policy and safeguarding consistency when it comes to the application of EC competition law.

44. According to Article 11(4) of the Council Regulation, no later than 30 days before the adoption of a decision applying Articles 81 or 82 of the Treaty and requiring that an infringement be brought to an end, accepting commitments or withdrawing the benefit of a block exemption regulation, NCAs shall inform the Commission. They have to send to the Commission, at the latest 30 days before the adoption of the decision, a summary of the case, the envisaged decision or, in the absence thereof, any other document indicating the proposed course of action.

45. As under Article 11(3) of the Council Regulation, the obligation is to inform the Commission, but the information may be shared by the NCA informing the Commission with the other members of the network.

46. Where an NCA has informed the Commission pursuant to Article 11(4) of the Council Regulation and the 30 days deadline has expired, the decision can be adopted as long as the Commission has not initiated proceedings. The Commission may make written observations on the case before the adoption of the decision by the NCA. The NCA and the Commission will make the appropriate efforts to ensure the consistent application of Community law […]

49. All members of the network should inform each other about the closure of their procedures which have been notified to the network pursuant to Article 11(2) and (3) of the Council Regulation […]

3.2. The initiation of proceedings by the Commission under Article 11(6) of the Council Regulation

51. Article 11(6) of the Council Regulation states that the initiation by the Commission of proceedings for the adoption of a decision under the Council Regulation shall relieve all NCAs of their competence to apply Articles 81 and 82 of the Treaty. This means that once the Commission has opened proceedings, NCAs cannot act under the same legal basis against the same agreement(s) or practice(s) by the same undertaking(s) on the same relevant geographic and product market. […]

4. THE ROLE AND THE FUNCTIONING OF THE ADVISORY COMMITTEE IN THE NEW SYSTEM

58. The Advisory Committee is the forum where experts from the various competition authorities discuss individual cases and general issues of Community competition law.

---

European Commission, Enhancing competition enforcement by the Member States’ competition authorities: institutional and procedural issues (2014)\(^{110}\)

7. This document reports on the initiatives which have been taken by way of follow up to the Report on the functioning of Regulation 1/2003 of 2009. Moreover, it analyses a range of areas that: (1) were not addressed by Regulation 1/2003; (2) were addressed in a general way while a need for a detailed response has subsequently arisen in practice or; (3) have emerged as new issues. […]

39. The position of the NCAs has evolved in the direction of more autonomy and effectiveness and many national laws already contain specific safeguards to ensure the independence and impartiality of NCAs. Such guarantees emphasize their importance for effective competition enforcement, strengthen the NCAs’ position vis-à-vis the Member States and very importantly strengthen the legitimacy of their action vis-à-vis stakeholders, including national parliaments and citizens. However, there are no explicit requirements in EU

---

law to ensure: (1) minimum guarantees of independence so that NCAs are able to execute their tasks in an impartial and independent manner; and (2) the effective and sustained operation of NCAs by means of sufficient human and financial resources.

40. As set out in the Communication, it is necessary to ensure that NCAs can execute their tasks in an impartial and independent manner. For this purpose, minimum guarantees are needed to ensure the independence of NCAs and their management or board members and to have NCAs endowed with sufficient human and financial resources. Important aspects in this respect are the grant of a separate budget with budgetary autonomy for NCAs, clear and transparent appointment procedures for the NCA's management or board members on the basis of merit, guarantees ensuring that dismissals can only take place on objective grounds unrelated to the decision-making of the NCA and rules on conflicts of interest and incompatibilities for the NCA's management or board. […]

52. Importantly, multilateral work within the ECN has been a major catalyst in encouraging Member States and/or NCAs to ensure greater convergence. This has resulted in the production of comparative reports as well as policy and guidance documents aimed at enhancing convergence in the areas of procedures, leniency and fines, as is explained further below.

53. However, there are limits to what can be achieved by voluntary convergence and 'soft tools' developed in the ECN, as well as the means to foster convergence in the context of cross-cutting EU programmes. Where procedural differences are rooted in national legal traditions, national fundamental right standards or other general principles, it may be difficult to achieve convergence with a common standard through the use of 'soft tools', including in the context of economic adjustment programmes. For example, in Ireland, the NCA does not have the ability to seek the imposition of civil/administrative fines for the breach of either EU or national competition rules. It can do so solely in criminal proceedings, involving trial by jury which in practice means that prosecutions are only brought against hard-core cartels. In view of avoiding any situation of under-enforcement of the competition rules in Ireland, a provision in the MoU with Ireland tried to address this issue. However, it appears that the power to impose civil/administrative sanctions will only be introduced if this would be made mandatory through EU legislation. […]

55. By way of follow up to the 2009 Report on Regulation 1/2003, the ECN made a detailed inventory of the investigation and decision-making procedures for competition enforcement which exist in the Member States. The Reports, which were published in November 2012, provided a clear overview of the status quo in the ECN for the first time.

56. […] while these soft tools cannot overcome constitutional impediments, obstacles flowing from national legal traditions or from national case law, the Recommendations show that there is a considerable degree of consensus within the ECN on the procedural tools which authorities must have to be able to effectively apply competition law. […]

60. In conclusion, despite the absence of explicit requirements in EU law for the procedures used by NCAs when applying the EU competition rules, voluntary convergence with the procedures set out for the Commission in Regulation 1/2003 has occurred in virtually all jurisdictions. However, the degree of convergence on procedures differs and divergence subsists even for some fundamental powers. This means that while some NCAs are better equipped than others, the vast majority do not have a complete set of powers at their disposal to apply Articles 101 and 102 TFEU, which are comprehensive in scope and are effective in all respects. This impinges on the ability of NCAs to effectively apply the EU competition rules. Soft tools developed within the ECN are helpful in facilitating further convergence, but not where divergences are rooted in constitutional rules or national legal traditions. Undertakings operating cross-border incur costs in terms of acquainting themselves with the different procedural rules which apply in different jurisdictions. Divergences in procedures also reduce predictability for such businesses. Another issue of concern is that achievements made to date are fragile as there is nothing to prevent changes in national laws or practices that weaken the powers of the NCAs.

61. As set out in the Communication, it is necessary to ensure that all NCAs have a complete set of powers at their disposal, which are comprehensive in scope and are effective. Important elements are the core investigative powers, the right of NCAs to set enforcement priorities, key decision-making powers and the necessary enforcement and fining powers to compel compliance with investigative and decision-making powers. […]

77. As set out in the Communication, in order to make enforcement of the EU antitrust rules more convergent and effective throughout the EU, it is necessary to ensure that all NCAs have effective powers to impose deterrent fines on undertakings and on associations of undertakings. Important aspects in this regard are
ensuring that NCAs can impose effective civil/administrative fines on undertakings and associations of undertakings for breaches of the EU competition rules; ensuring that basic fining rules are in place taking into account gravity and duration of the infringement and foreseeing a uniform legal maximum; and ensuring that fines can be imposed on undertakings, in line with the constant case law of the EU courts, in particular, on issues such as parental liability and succession. Any measures taken to this end would need to find the right balance between increased convergence of the basic rules for fines and an appropriate degree of flexibility for NCAs when imposing fines in individual cases.

Further to the firmness of the legal basis, the cooperation within competition law has proven to be a particularly useful model over the last 15 years. Its success is largely based on the enforcement model designed by Regulation 1/2003 and the Commission Notice on cooperation within the Network of Competition Authorities, which very much rely on and encourage the decentralised application of some substantive legal rules. A fundamental factor is that such rules are unified for all EU Member States. As a consequence, there was a need to ensure the consistency mechanism within the ECN, thus avoiding the concepts of the EU competition law being applied differently at the Member State level. On the other hand, the CJEU retains the main role in interpreting such rules, and the Commission of strong and central enforcer of EU competition law, tackling cases with the typically biggest impact and setting the tone for the development of EU competition law within ECN.

The fact that it is also the Commission, which is also the enforcer, that provides the logistical support to the ECN, i.e. it coordinates the exchange of information, ensures linguistic competence, organises the meeting of advisory boards, etc., is not without the impact on overall functioning and development of this model of cooperation. The cooperation within ECN has led to a considerable level of convergence between Member States’ administrative procedures and procedural practices. The recent 2014 Communication from the Commission clearly illustrates, however, that certain differences between organisation of NCAs, their powers and applied procedures might still have an adverse impact on consistency and legal certainty, and – when those differences derive from different legal traditions – it might not be possible to have them overcome by a soft law approach.

(b) Use of technology

Kekelekis advocates that the most important element that has come from the creation of the ECN is a “can do” attitude, and the way it has been embraced by all Member States and the willingness shown by all to attempt to accommodate each other and to share information when necessary (2009, 37–39). The efficient use of ICTs contributes to its success.


The ECN provides a valuable forum for discussion and cooperation among the NCAs. NCAs can now learn from each others’ experiences, coordinate investigations, help each other with investigations, exchange evidence and information and discuss issues of common interest. Thanks to the ECN’s interactive access and the electronic database containing details from the standard forms, NCAs can also be informed of other authorities’ main contact persons. The ECN thus makes it possible for NCAs to identify among themselves who does what. It is not therefore a simple electronic connection; it is rather an effective daily working tool, an open network that allows, on the one hand, an exchange of confidential information and, on the other hand, easy interaction between the members of the network. Consequently, cooperation can occur even in the absence of formal procedures or formal requirements.

Article 11(3) of the Regulation creates an obligation for all NCAs to inform the Commission before or without delay after commencing the first formal investigative measure in all cases involving the application of Article 81 and 82 TEC. This information may be shared with other NCAs.

“In practice, the obligation to inform about new cases is complied with by uploading the relevant information in a common case-management system. This system was developed by the DG COMP IT-team and has been operational from 1 May 2004. The system is secured against unauthorised access and access rights are restricted to case-handlers and other authorised personnel of the competition authorities. The IT-system foresees the possibility to insert standardized information on, for instance, the parties, the products, the territories, the alleged infringement, its suspected duration, the contact details of the case handlers in charge etc. […]”
2.5 Criminal justice cooperation

2.5.1 Legal framework

Past

- Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention)\textsuperscript{111}
- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems\textsuperscript{112}

In force

- Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA)\textsuperscript{113}
- Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters\textsuperscript{114}
- Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings\textsuperscript{115}
- Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters\textsuperscript{117}

Actors

(a) Eurojust

- Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA)\textsuperscript{118}
- Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime\textsuperscript{119}
- Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime\textsuperscript{120}
- Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust)\textsuperscript{121}

(b) Europol


(c) European Public Prosecutor’s Office (EPPO)

- Proposal for a Council Regulation on the establishment of the European Public Prosecutor’s Office\textsuperscript{124}

\textsuperscript{111} OJ C 316, 27.11.1995, pp. 1–32.
\textsuperscript{112} OJ L 69, 16.03.2005, pp. 67–71.
\textsuperscript{116} OJ L 218, 14.08.2013, pp. 8–14.
\textsuperscript{117} OJ L 130, 01.05.2014, pp. 1–36.
\textsuperscript{118} OJ L 63, 06.03.2002, pp. 1–13.
\textsuperscript{119} OJ L 245, 29.09.2003, pp. 44–45.
\textsuperscript{120} OJ L 138, 04.06.2009, pp. 14–32.
\textsuperscript{121} COM(2013) 535 final.
\textsuperscript{122} OJ L 121, 15.05.2009, pp. 37–66.
\textsuperscript{123} COM(2013) 173 final.
\textsuperscript{124} COM(2013) 534 final.
2.5.2 General overview

(a) European Arrest Warrant (EAW)

The European Arrest Warrant (EAW) constitutes the leading and arguably the only successful instrument adopted pursuant to the principle of mutual recognition in criminal justice matters in the EU. According to article 82(1) TFEU, “[j]udicial cooperation in criminal matters in the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States in the areas referred to in paragraph 2 and in Article 83.” In particular, section (a) of the same article refers to the need to adopt rules in order to ensure the mutual recognition of judgments.

The EAW entered into force on 1 January 2004, following a period of extremely brief negotiations. Its adoption process was significantly accelerated by the events of 9/11. The Council of Ministers agreed on a draft text for the EAW on 10 December 2001, a mere three months after the Commission presented its proposal. Six months later, in June 2002, the instrument was adopted.

The main goal of the EAW is to expedite the extradition process by reducing the grounds for refusal, while at the same time minimising cumbersome requirements and political influence, and by doing so maximising efficiency. Before the EAW, extradition between EU Member States occurred on the basis of the European Convention on Extradition. This was a move away from the more traditional, international-agreement-based extradition procedure that was in place prior to the EAW. The most important changes brought about by the EAW, compared to the traditional interstate framework, are:

1. The removal of the executive branch from the extradition proceedings. The transfer of suspected and convicted persons on the basis of the EAW takes place between judicial authorities.
2. The procedure is of a summary nature, based on a standardised form (the EAW) and not on the evidence which underlies the warrant.
3. The procedure is subject to strict and short time limits and ‘shall be dealt with and executed as a matter of urgency’, the instrument requires a final decision on surrender within ten days in case the person wanted consents, in other cases this is 60 days.
4. The so called 'double-criminality' requirement is abolished for a list of 32 offences, provided that they are punishable for a maximum period of at least three years’ imprisonment in the issuing state. Offences not included on this list are subject to a requirement of double-criminality; in case of wanted suspects when they are punishable in the issuing state by a custodial sentence or a detention order for a maximum period of at least twelve months, and in case of wanted convicts for sentences of at least four months.
5. The number of grounds that a state can invoke to refuse to execute a EAW has been limited to three obligatory grounds and seven optional grounds (i.e. states can choose to include these in their national legislation).


**Article 3**

**Grounds for mandatory non-execution of the European arrest warrant**

The judicial authority of the Member State of execution (hereinafter "executing judicial authority") shall refuse to execute the European arrest warrant in the following cases:

1. if the offence on which the arrest warrant is based is covered by amnesty in the executing Member State, where that State had jurisdiction to prosecute the offence under its own criminal law;
2. if the executing judicial authority is informed that the requested person has been finally judged by a Member State in respect of the same acts provided that, where there has been sentence, the sentence has been served or is currently being served or may no longer be executed under the law of the sentencing Member State;
3. if the person who is the subject of the European arrest warrant may not, owing to his age, be held criminally responsible for the acts on which the arrest warrant is based under the law of the executing State.

**Article 4**

**Grounds for optional non-execution of the European arrest warrant**

The executing judicial authority may refuse to execute the European arrest warrant:

1. if, in one of the cases referred to in Article 2(4), the act on which the European arrest warrant is based does not constitute an offence under the law of the executing Member State; however, in relation to taxes or duties, customs and exchange, execution of the European arrest warrant shall not be refused on the ground that the law of the executing Member State does not impose the same kind of tax or duty or does not contain the same type of rules as regards taxes, duties and customs and exchange regulations as the law of the issuing Member State;
2. where the person who is the subject of the European arrest warrant is being prosecuted in the executing Member State for the same act as that on which the European arrest warrant is based;
3. where the judicial authorities of the executing Member State have decided either not to prosecute for the offence on which the European arrest warrant is based or to halt proceedings, or where a final judgment has been passed upon the requested person in a Member State, in respect of the same acts, which prevents further proceedings;
4. where the criminal prosecution or punishment of the requested person is statute-barred according to the law of the executing Member State and the acts fall within the jurisdiction of that Member State under its own criminal law;
5. if the executing judicial authority is informed that the requested person has been finally judged by a third State in respect of the same acts provided that, where there has been sentence, the sentence has been served or is currently being served or may no longer be executed under the law of the sentencing country;
6. if the European arrest warrant has been issued for the purposes of execution of a custodial sentence or detention order, where the requested person is staying in, or is a national or a resident of the executing Member State and that State undertakes to execute the sentence or detention order in accordance with its domestic law;
7. where the European arrest warrant relates to offences which:
   (a) are regarded by the law of the executing Member State as having been committed in whole or in part in the territory of the executing Member State or in a place treated as such; or
   (b) have been committed outside the territory of the issuing Member State and the law of the executing Member State does not allow prosecution for the same offences when committed outside its territory.

Moreover, three grounds for refusal that traditionally figure prominently in the law of extradition are absent from the EAW: (a) the offence is ‘political’, (b) the offence is ‘fiscal’, and (c) the person sought is a national of the requested state.

(b) European Evidence Warrant

After a series of long and cumbersome negotiations, the European Evidence Warrant (EEW) was adopted in 2008, but the instrument has been largely ignored by Member States. Part of the explanation is that the experience with the European Arrest Warrant, i.e. a loss of sovereignty not necessarily coupled with fundamental rights guarantees, led to a stricter drafting of the instrument on the EEW. This, in combination with the limited scope of the instrument – does not provide for a mechanism to gather new evidence- have led to its limited success.

(c) European Investigation Order

The conclusion that can be drawn from the experience of the European Evidence Warrant is that Member States have not been willing to further their cooperation in criminal justice matters or to give up further parts of their national sovereignty, due to the experiences generated by the adoption of the European Arrest Warrant. Yet, the newly introduced instrument, the European Investigation Order, addresses some of the concerns that Member States raised regarding the EAW.

Directive 2014/41/EU regarding the European Investigation Order in criminal matters was adopted in 2014 with a view to be implemented by 22 May 2017. A common approach concerning a vital area of judicial cooperation, the exchange of evidence, is arguably a necessity. Indeed, Member States already cooperate widely in the gathering and collection of evidence in trans-border cases, and a comprehensive, unified regulatory framework is expected to simplify matters. One caveat is that for such a measure to be successful, Member States have to demonstrate not only a strong willingness to implement, but also to adopt a measure, while they are still at the negotiating table.

(d) Eurojust

Eurojust is an illustrative example of the establishment of a successful coordination mechanism between law enforcement authorities at the EU level. Set up in 2002, and entrusted with the task of strengthening the fight against cross-border and organised crime, it is presently an EU body with legal personality and
its seat is located in the Hague. The primary aim of Eurojust is facilitating and stimulating cooperation between the 'competent authorities' of the 28 EU Member States.

**Treaty on the Functioning of the European Union (1957, as amended 2007)**

**Article 85**

1. 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 Member States or requiring a prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities and by Europol.

In this context, the European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Eurojust’s structure, operation, field of action and tasks. These tasks may include:

(a) the initiation of criminal investigations, as well as proposing the initiation of prosecutions conducted by competent national authorities, particularly those relating to offences against the financial interests of the Union;
(b) the coordination of investigations and prosecutions referred to in point (a);
(c) the strengthening of judicial cooperation, including by resolution of conflicts of jurisdiction and by close cooperation with the European Judicial Network.

These regulations shall also determine arrangements for involving the European Parliament and national Parliaments in the evaluation of Eurojust’s activities. […]

Eurojust was founded in order to serve the following objectives: (1) counter serious and organised crime within the EU; (2) increase the level of safety and security of EU citizens; (3) stimulate judicial cooperation between EU Member States; and (4) address the need for a body that could cooperate with the European Judicial Network (EJN).

The legal framework applicable to Eurojust was lastly amended in 2009. It resulted to Eurojust's empowerment while at the same time creating the necessary preconditions for the successful accommodation of any possible future expansion thereof.

Eurojust is composed of criminal justice experts that represent their Member State of origin (‘national correspondents’) and their activity is complemented by deputies and assistants. Each national member is seconded by the Member State in accordance with its legal system, be that a prosecutor, judge or police officer of equivalent competence. The duration of their function is for a maximum of four years and is not renewable. The statute of the national members (and their employees) forms part of the national law of the Member State concerned. National correspondents as a whole form “the College”, an organ responsible for the organisation and the operation of Eurojust. The College can act collectively, but also through one or more national correspondents. Each correspondent has one vote in the College.

The primary aim of Eurojust's competences is to stimulate, improve and coordinate cooperation between national authorities. The most important competence of Eurojust lies in providing assistance to an investigation and prosecution of serious, organised and/or cross-border crime, either on its own initiative, or following a request by an EU Member State. It provides support to these authorities whenever they are in need for it, in cases concerning two or more EU Member States. In addition, Eurojust can assist investigations or prosecution that is of concern to a single Member State and the EU, if either the Commission or the Member State itself has requested for this assistance.

Eurojust’s general competence covers only serious, organised cross-border crime, for which a certain threshold has to be met. Examples of such types of crime are cybercrime, fraud, corruption, money laundering, environmental crimes and criminal organisations.

An exception to the aforementioned general rule is cooperation in cases of child protection. Eurojust has the authority to 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 centre of expertise in judicial cooperation in cases concerning children”.

It shall be available to support and advise the national correspondents when dealing with cases involving children. Focusing on issues important to Eurojust and its partners in the Member States, the contact point is for a maximum of four years.

---

Criminal justice cooperation

point is expected to raise awareness on child protection-related matters, disseminate relevant information and advice on the possible actions to be taken.

Eurojust can, either through its national members or through the College, request the authorities of EU Member States to start an investigation or prosecution, accept that another state is in a better position to start an investigation or prosecution, set up a joint investigation team (JIT), and/or provide all the information relevant for a JIT to fulfil its tasks. Furthermore, Eurojust can request national authorities to initiate certain investigative measures and other measures that are justified for the purpose of a prosecution of criminal activities.

Eurojust may act in the interest of fostering cooperation among Member States in the judicial field, as well as in the interest of removing obstacles to such cooperation. The competent authority of a Member State may report to Eurojust refusals or obstacles concerning the execution of a request for, or decision on, judicial cooperation due to the uncooperative attitude of authorities in other Member States. In this circumstance, Eurojust, acting as a College, may issue a written opinion on the matter and forward it to the national authorities concerned. Although this opinion is of a non-binding nature, it is nonetheless able to solve a controversy and smooth cooperation among the parties concerned.

None of Eurojust’s decisions are binding in nature. Eurojust may assert an advisory role towards national authorities. It is also in a position to provide assistance of a more ‘logistical’ nature, such as interpretation and translation. Nevertheless, the non-binding nature of its advisory acts lies at the heart of its success as a unit entrusted with the task to promote cooperation in criminal matters. Indeed, Member States benefit from the contacts and the network that has been put in place by Eurojust, in order to effectively cooperate in criminal investigations, while maintaining their sovereignty or competence over criminal matters intact.

(e) A proposal for the European Public Prosecutor’s Office (EPPO)

Treaty on the Functioning of the European Union (1957, as amended 2007)

Article 86

1. In order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor’s Office from Eurojust. The Council shall act unanimously after obtaining the consent of the European Parliament.

In the absence of unanimity in the Council, a group of at least nine Member States may request that the draft regulation be referred to the European Council. In that case, the procedure in the Council shall be suspended. After discussion, and in case of a consensus, the European Council shall, within four months of this suspension, refer the draft back to the Council for adoption.

Within the same timeframe, in case of disagreement, and if at least nine Member States wish to establish enhanced cooperation on the basis of the draft regulation concerned, they shall notify the European Parliament, the Council and the Commission accordingly. In such a case, the authorisation to proceed with enhanced cooperation referred to in Article 20(2) of the Treaty on European Union and Article 329(1) of this Treaty shall be deemed to be granted and the provisions on enhanced cooperation shall apply.

2. The European Public Prosecutor’s Office shall be responsible for investigating, prosecuting and bringing to judgment, where appropriate in liaison with Europol, the perpetrators of, and accomplices in, offences against the Union's financial interests, as determined by the regulation provided for in paragraph 1. It shall exercise the functions of prosecutor in the competent courts of the Member States in relation to such offences.

3. The regulations referred to in paragraph 1 shall determine the general rules applicable to the European Public Prosecutor's Office, the conditions governing the performance of its functions, the rules of procedure applicable to its activities, as well as those governing the admissibility of evidence, and the rules applicable to the judicial review of procedural measures taken by it in the performance of its functions.

4. The European Council may, at the same time or subsequently, adopt a decision amending paragraph 1 in order to extend the powers of the European Public Prosecutor’s Office to include serious crime having a cross-border dimension and amending accordingly paragraph 2 as regards the perpetrators of, and accomplices in, serious crimes affecting more than one Member State. The European Council shall act unanimously after obtaining the consent of the European Parliament and after consulting the Commission.

Art 86 TFEU envisages the establishment of the European Public Prosecutor's Office (EPPO), originating from Eurojust. The idea of a European prosecutor is not fresh, but dates back to the so-called ‘Corpus
Criminal justice cooperation

Iuris’ project, during the 1990s.\textsuperscript{127} The core idea was that (a very limited) European code dealing with the protection of European Union financial interests would be enforced by a dedicated EU prosecutor, active across the territory of the EU. These proposals were regarded as far too ambitious at that time and eventually were shelved.

The current version of the EPPO has taken into account the aforementioned concern and, thus, represents an even further watered down version of the original proposal. The establishment and functioning of an EPPO would be realized through Council regulations (thus, not by means of the ordinary legislative procedure). Yet, even in its current form, it remains controversial. This is evidenced by a ‘yellow card’ issued by fourteen national parliaments. Therefore, at the time of writing, the future of the project remains uncertain.\textsuperscript{128}

\textbf{(f) Europol}

\textbf{Treaty on the Functioning of the European Union (1957, as amended 2007)}

\textbf{Article 87}

1. The Union shall establish police cooperation involving all the Member States’ competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences. […]

\textbf{Article 88}

1. Europol’s mission shall be to support and strengthen action by the Member States’ police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

2. The European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Europol’s structure, operation, field of action and tasks. These tasks may include:

(a) the collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of the Member States or third countries or bodies;

(b) the coordination, organisation and implementation of investigative and operational action carried out jointly with the Member States’ competent authorities or in the context of joint investigative teams, where appropriate in liaison with Eurojust.

These regulations shall also lay down the procedures for scrutiny of Europol’s activities by the European Parliament, together with national Parliaments.

3. Any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member State or States whose territory is concerned. The application of coercive measures shall be the exclusive responsibility of the competent national authorities.

The legal basis that enabled the creation of a European Police Office (Europol), as part of police and judicial cooperation in criminal matters in the EU, was introduced in 1992 by the Maastricht Treaty. Europol gained its formal status by means of the 1995 Europol Convention. The organisation became operational in 1999 and it currently runs on the basis of the 2009 Europol Decision.

According to Art 2(1) of the Europol Convention, the initial objective of Europol was to support the competent authorities of the Member States in their efforts to prevent and combat terrorism, unlawful drug trafficking and other forms of serious international crimes. Europol’s core task is to support the police authorities of the Member States in their intelligence work. It has to notify the competent Member State authorities of the existence of information concerning their investigations and of the connections identified between criminal offences.

Although Europol was initially founded as an inter-governmental organisation, it has, in the post-Lisbon era, been mainstreamed under Art 88 TFEU. The Europol Convention of 1995 has been supplemented by

\textsuperscript{127} Cf. http://www.eppo-project.eu.

three Protocols and later a Council Decision. Its role has developed over the years, both in terms of scope and powers.

Police cooperation has been recognised as a Union objective in Art 87 TFEU, while Art 88 TFEU specifies Europol's role in supporting national criminal law enforcement in relation to "serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy". This should be assessed in comparison to its original mandate, which was concerned solely with organised crime. Art 88(2) TFEU sets out its two main policy fields: intelligence related (collection, storage, processing, analysis and exchange of information) and investigative and operational competences, carried out jointly with Member States' authorities.

Europol is not entitled to exercise direct executive powers in Member States. Europol's task is to support national police forces and it is not an independent police force per se. Its competence is limited in comparison to other bodies of this nature, such as the American Federal Bureau of Investigation. It has, however, the authority to cooperate with the national police forces whenever the case in question requires a common approach by Member States due to "the scale, significance and consequences of the offences".129

Europol's staff in the Hague support and coordinate law enforcement activities conducted in Member States. The cooperation network of Europol is comprised by a centralised headquarter established in the Hague, national units and liaison officers. The national units are established by Member States, who also appoint the head of each national unit. National units liaise between Europol and the competent authorities of Member States. In particular, they supply Europol with relevant information and intelligence; respond to Europol's requests for information, intelligence and advice; keep information and intelligence up to date; evaluate and transmit information and intelligence to national competent authorities; request Europol advice, information, intelligence and analysis. At least one person from each national unit is seconded to Europol as a liaison officer in order to strengthen cooperation among them. Liaison officers represent the interest of national units within Europol and constitute the "national liaison bureaux at Europol". Their main role consists in the exchange of information and intelligence between their national unit and Europol.

(g) Protection of personal data in criminal justice cooperation

The protection of personal data in criminal justice cooperation is based on two pillars, i.e. access rights for data subjects and oversight by a dedicated joint supervisory body. However, these two pillars operate differently in case of Eurojust and Europol. The following paragraphs will critically assess the framework applicable in both bodies.

i) Eurojust

Although the processing of personal data by Eurojust follows the 'general' norms set out by the 1995 Data Protection Directive, a specific regime has been put in place for exercising data subjects' rights. In particular, the Eurojust Decision establishes an ad hoc procedure for the exercise of the right of access to personal data processed by this institution. In order to obtain access to her personal data, the data subject needs to contact the national correspondent established in his Member State. In turn, this national contact point has to refer the access request to Eurojust 'without delay'. The exercise of the right of access is free of charge. The national contact point who receives the request should process it in accordance with the law and the procedures applicable in the Member State which receives the individual's request, unless the data subject's personal data were processed by another contact point of another Member State.

An access request may be denied in certain cases, namely if an access request "may jeopardise one of Eurojust’s activities", "any national investigation" or "the rights and freedoms of third parties". In any event, the data subject's request should be dealt with within three months of receipt. The ad-hoc regime with regard to the exercise of access rights in the framework of Eurojust is also of relevance to the exercise of the right of appeal against a decision made by Eurojust. In this case the data subject has to contact an ad hoc body, the Joint Supervisory Body (JSB).

The Eurojust JSB is an independent body entrusted with the task to ensure that Eurojust processes personal data in accordance with the Eurojust Decision. Although a DPA does not handle claims that concern the processing of personal data by Eurojust, the JSB provides equivalent guarantees of independence and impartiality, mainly due its structure. The JSB is composed of judges or other members with an equal level of independence that are not members of Eurojust. A representative of each Member

129 Art 4(1) Europol Decision.
State seats in the JSB and three of its members are appointed as permanent members for a period of three years. The JSB is entitled to a full access to all files containing personal data and Europol is obliged to provide the JSB with all the information requested. Apart from asserting the role of an appellate body in cases in which the data subject challenges a decision taken by Europol, the JSB also monitors the data processing activities carried out by Europol. The JSB is also the point of contact responsible with receiving requests by data subjects that are not satisfied with a decision of Europol concerning the correction or deletion of their personal data. The Eurojust Decision states that in this case the matter can be referred to the JSB “within thirty days of receiving Eurojust’s decision”. The JSB adopts binding decisions against such processing activities, which Eurojust is obliged to follow.

ii) Europol

Individuals whose personal data are processed by Europol also have the right to gain access to them, as well as correct or delete any incorrect data. Any person willing to exercise the right of access needs to address a request to this effect to the national DPA. The request should be introduced “without excessive costs” for the data subject. Once the national DPA receives such request, it shall refer it to Europol “without delay, and in any case within one month of receipt”. In turn, Europol needs to reply to the request within “without undue delay and in any case within three months of its receipt by Europol”. Before deciding on such a request, Europol consults the competent national DPA. Although the procedure established by the Europol Decision for accessing personal data is more articulated for the data subject than the ‘ordinary’ procedure set by 1995 Data Protection Directive, it is noteworthy that the exercise of access rights in the case of Europol follows a certain timeframe established by the EU legislator. Apart from respecting the data subject’s interest to obtain a reply to his access request, the time limits ensure that national DPAs and Europol cooperate among each other in a timely and effective manner.

Pursuant to the Europol Decision, an access request may be refused in the following circumstances: when such refusal is necessary to enable Europol to fulfil its tasks properly (1); when it is necessary to protect security and public order in Member States or to prevent crime (2); when the refusal is necessary to guarantee that any national investigation will not be jeopardised (3); to protect the rights and freedoms of third parties (4). If the data subject does not find itself in agreement with Europol’s reply to an access request or if there has been no response to his request within the designated time limit, he may appeal to the Joint Supervisory Body (JSB). Hence, the JSB will assess the case concerned and then make a decision “in close cooperation” with the national DPA that handled the case as first.

As in the case of Eurojust, the JSB of Europol is an independent body to ensure that the processing of personal data by Europol is lawful and legitimate and that data subjects’ rights are not violated. But its composition is different from the one of Eurojust. The JSB is composed of a maximum of two members or representatives from each national DPA. They are appointed by their respective Member States for a period of five years. Europol has to cooperate with the JSB by supplying the information it requests and by providing it with access to documents, paper files and data stored in data files. Europol is obliged to implement the decisions of the JSB on appeals and to adopt its solutions to existing problems relating to the functioning Europol.

In 2013 the European Commission tabled a proposal for reforming the Europol Decision. Among others, the proposal aims at strengthening the protection of personal data. The proposal would abolish Europol JSB and empower EDPS to supervise Europol’s data processing operations.

The main measures envisaged are:

- further strengthening of the existing autonomous EUROPOL data protection regime: the principles underpinning Regulation (EC) No 45/2001 on the protection of individual with regard to processing of personal data by the Community institutions and bodies and on the free movement of such data will be drawn upon to a greater extent. EUROPOL’s data protection rules have been aligned with other data protection instruments applicable in the area of police and judicial cooperation, while taking into due account the specificity of law enforcement;
access by Member States to personal data held by Europol and relating to operational analyses, is made indirect based on a hit/no hit system: an automated comparison produces an anonymous ‘hit’ if the data held by the requesting Member State match data held by EUROPOL. The related personal or case data are only provided in response to a separate follow-up request;

restrictions on the processing of certain data: the processing of personal data on victims, witnesses, persons different from suspects, and minors is prohibited unless strictly necessary. This limitation also applies to data revealing racial or ethnic origin, political opinions, religions or beliefs, trade-union membership and of data concerning health or sex life (sensitive personal data). Furthermore, sensitive personal data can only be processed where they supplement other personal data already processed by Europol. Europol is obliged to provide every six months an overview of all sensitive personal data to the EDPS. Lastly, no decision which produces legal effects concerning a data subject can be taken solely on the basis of automated processing of sensitive personal data, unless it is authorised by EU or national law or by the EDPS;

reinforced right of access: to increase transparency, individuals’ right of access to personal data held by Europol is reinforced;

clear rules on the division of responsibility in regard to data protection: Europol would be responsible for reviewing the continuing need to store personal data at regular intervals;

obligation of logging and documentation: to ensure better control over the use of data and clarity on who has been processing it, the proposed Regulation would prohibit modification of the logs;

right to recourse: any individual could turn to Europol for compensation for unlawful data processing or an action incompatible with the provisions of this proposed Regulation;

strengthened role of EUROPOL’s external data protection supervisory authority: the European Data Protection Supervisor will be competent for the supervision of processing of personal data by Europol. The national data protection authorities, however, remain competent for supervision of input, the retrieval and any communication to Europol of personal data by the Member State concerned;

joint supervision: the proposal introduces elements of “joint supervision” on data transferred to and processed at Europol. It is stipulated that the European Data Protection Supervisor and national supervisory authorities, each acting within its competences, should co-operate with each other.

2.5.3 Observations

(a) National differences

Paul De Hert and Auke Willems, “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?” (2015)132

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

---

132 Original footnotes omitted.
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 […]. 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 […] 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.

(b) Extraterritoriality

i) Conflicts of jurisdiction

An important question in criminal justice cooperation (in case of trans-border crime) is how to deal with conflicts of jurisdiction. Conflicts of jurisdiction are neither positive nor 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 required. In the former, coordination takes the form of establishing which state would be best positioned to deal with the case and in the later of ensuring that the alleged crime does not go unpunished due to a lack of interest to prosecute, which is often a political question.
Jurisdiction is a state’s power to exercise authority over persons and entities within its territory. It can be broadly categorized into three types. The first is prescriptive jurisdiction, which is the state’s power to legislate (as well as to amend or repeal legislation). The second is enforcement jurisdiction; the power of a state to enforce its legislation, e.g. the police and prosecution by investigating crimes and arresting suspects. The third is adjudicative jurisdiction, exercised when national courts, tribunals and other bodies exercise judicial functions to rule on disputes, or adjudicate.\(^{133}\)

The first and foremost principle on which jurisdiction is based is 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 states exercising jurisdiction.

In addition to territorial jurisdiction, there can also be extraterritorial jurisdiction, employed by states to expand their jurisdiction beyond territorial boundaries. Conflicting claims of jurisdiction arise when extraterritorial jurisdiction over the same alleged crime is simultaneously claimed by more than one states. If jurisdiction were solely based on the territoriality principle, only one state would be in a position to bring charges and hence, such conflicts would not arise.

Extraterritorial 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 they all have in common is that a state exercises its criminal jurisdiction over a crime committed (partially) outside its territory.

Because of the existence of extraterritorial grounds for jurisdiction, in combination with the increasing cross-border nature of crime, it is very well possible that two states claim jurisdiction over the same (alleged) crime.

It is therefore important for states 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 designed to address the 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 often involves a political process by which states can use (sometimes binding) guidelines contained in (bilateral) treaties (often these are extradition treaties). As far as the EU is concerned, 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.

A negative conflict of jurisdiction could lead to impunity. This situation is of course especially problematic with regard to alleged perpetrators of serious international crimes. A similar situation may arise when countries are not willing or capable to prosecute. International initiatives to establish international ad hoc courts (like the Rwanda Tribunal set up by the United Nations [UN]) or a permanent court (like the International Criminal Court [ICC]) can offer relief for certain categories of the most serious crimes. The principle of complementarity in the Rome Treaty on the ICC is also of interest; this court’s jurisdiction is complementary to national criminal jurisdictions, which means that states have the primary responsibility to investigate and prosecute and that the ICC acts as a court of last resort, in the sense that it only asserts jurisdiction when the 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 jurisdictions.

\[\text{ii) The 2009 Framework Decision on jurisdiction in criminal proceedings}\]

There is not one single text in international public law that deals with all aspects of jurisdiction in a comprehensive manner. At the EU level, an attempt is being made to devise such an instrument. In 2009, the EU agreed upon a framework decision on how to coordinate conflicting claims of jurisdiction between states. The framework decision aims to enhance judicial cooperation between EU Member States, in order to prevent unnecessary parallel criminal proceedings concerning the same facts and the same person.

The framework decision lays out a 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

\(^{133}\) Cf. Sect. 2.1.3(b).
consultations when parallel proceedings exist, in order to find a solution aimed at avoiding the negative consequences arising from these proceedings.

**Council Framework Decision on jurisdiction in criminal proceedings (2009)**

**CHAPTER 2 – EXCHANGE OF INFORMATION**

**Article 5**

**Obligation to contact**

1. 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.

2. If the contacting authority does not know the identity of the competent authority to be contacted, it shall make all necessary inquiries, including via the contact points of the European Judicial Network, in order to obtain the details of that competent authority.

3. The procedure of contacting shall not apply when the competent authorities conducting parallel proceedings have already been informed of the existence of these proceedings by any other means.

**Article 6**

**Obligation to reply**

1. The contacted authority shall reply to a request submitted in accordance with Article 5(1) within any reasonable deadline indicated by the contacting authority, or, if no deadline has been indicated, without undue delay, and inform the contacting authority whether parallel proceedings are taking place in its Member State. In cases where the contacting authority has informed the contacted authority that the suspected or accused person is held in provisional detention or custody, the latter authority shall treat the request as a matter of urgency.

2. If the contacted authority cannot provide a reply within any deadline set by the contacting authority, it shall promptly inform the contacting authority of the reasons thereof and indicate the deadline within which it shall provide the requested information.

3. If the authority which has been contacted by a contacting authority is not the competent authority under Article 4, it shall without undue delay transmit the request for information to the competent authority and shall inform the contacting authority accordingly.

**Article 7**

**Means of communication**

The contacting and contacted authorities shall communicate by any means whereby a written record can be produced.

If parallel proceedings exist, the relevant authorities shall enter into direct consultations in order to find a solution aimed at avoiding the negative consequences arising from these simultaneous proceedings. This may lead to concentrating the proceedings in one jurisdiction. When the relevant authorities enter into direct 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 it is appropriate and provided that it falls under its competence.

The 2009 Framework Decision provides for a useful tool for coordination between EU Member States. However, the instrument does not provide for a mandatory termination of parallel proceedings. On the contrary, it leaves it entirely to the discretion of the Member States whether to concentrate the proceedings in one state or to continue parallel proceedings. As a result, it creates the danger of imposing a double burden on suspects, and also transforms the proceedings into a race to reach decision first. The instrument, however, does provide some useful guidelines on how to deal with conflicts, which might offer relief to a suspect who is being tried in various jurisdictions. Nevertheless, it is silent on the topic of the defendants’ rights. These rights are not listed as a specific factor that needs to be taken into consideration when determining where best to prosecute a suspect. This underlines the instrument’s focus on prosecutorial intentions, since it mainly 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 Member States simply do not want to go this far and possibly surrender parts of their national sovereignty
as to where a suspect can be prosecuted, the current solution might offer the best of both worlds; efficient guidelines, but no loss of sovereignty.

iii) The 2013 Directive on attacks against information systems

To contrast the modest and non-binding arrangement of conflicts of jurisdiction in the 2009 Framework Decision, the 2013 Directive on attacks against information systems presents an example of a precise and more developed arrangement of jurisdiction in a specific area of law that naturally triggers competing claims of jurisdiction. The 2013 Directive replaces a former legal instrument on cybercrime, i.e. the 2005 framework decision on attacks against information systems.

The 2005 Framework Decision aimed to prevent and combat this relatively new form of criminal activity, which is effectively borderless, by enhancing the security of information infrastructures while at the same time providing law enforcement authorities with the means to act. To this end, the Framework Decision proposed the approximation of criminal law systems and the enhancement of cooperation between judicial authorities concerning:

- illegal access to information systems,
- illegal system interference, and
- illegal data interference.

In accordance with the Framework Decision, each Member State had jurisdiction for offences committed on its territory or by one of its nationals. Where several states have jurisdiction over one single offence, they must cooperate, in order to reach a decision as to which jurisdiction proceedings will be conducted against the perpetrator of the alleged offence. Member States would exchange all information intended to enhance cooperation. Notably, national operational points of contact, available twenty-four hours a day and seven days a week, would be appointed. The Framework Decision established an obligation for states to prosecute in case it does not extradite its own nationals. The Framework Decision also listed factors that should be taken into consideration in case one or more Member States have expressed a desire to prosecute:

<table>
<thead>
<tr>
<th>Framework Decision on attacks against information systems (2005)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Article 10</strong></td>
</tr>
<tr>
<td><strong>Jurisdiction</strong></td>
</tr>
<tr>
<td>4. 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:</td>
</tr>
<tr>
<td>- the Member State shall be that in the territory of which the offences have been committed according to paragraph 1(a) and paragraph 2,</td>
</tr>
<tr>
<td>- the Member State shall be that of which the perpetrator is a national,</td>
</tr>
<tr>
<td>- the Member State shall be that in which the perpetrator has been found.</td>
</tr>
</tbody>
</table>

The recently adopted 2013 Directive has furthered the approach by putting forward rules of cooperation for a specific type of offense, rather than a general instrument. This approach might prove more fruitful than the above-mentioned Framework Decision on jurisdictional conflicts, which covers a broad range of crimes, but does not set out any binding rules.

The 2013 Directive aims to replace and by this expand the provisions of the previous Framework Decision (in fact, in the interest of clarity, it replaces the framework decision in its entirety). The amendments are substantial and the nature of the new instrument offers advantages.

<table>
<thead>
<tr>
<th>Directive on attacks against information systems (2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Article 1</strong></td>
</tr>
<tr>
<td><strong>Subject matter</strong></td>
</tr>
<tr>
<td>This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the</td>
</tr>
</tbody>
</table>
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.

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 Art 12 on jurisdiction.

**Directive on attacks against information systems (2013)**

**Article 12**

**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.

The third paragraph of this provision obliges a Member State that decides to establish jurisdiction over an offence covered by the Directive to inform the Commission. The concept of enabling a third 'neutral' party to mediate between states in the event of conflicting claims of jurisdiction is a potentially powerful mechanism. However, the Directive does not go further than requiring Member States to 'inform' the Commission. If the Commission does not have any decision making power, or binding guidelines to determine what Member State is best positioned for prosecution, all it can provide is a mere recommendation.

**Article 12**

**Exchange of information**

1. 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.

2. Member States shall inform the Commission of their appointed point of contact referred to in paragraph 1. The Commission shall forward that information to the other Member States and competent specialised Union agencies and bodies.

3. Member States shall take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate the reporting of the offences referred to in Article 3 to 6 to the competent national authorities without undue delay.

Article 13 puts in place a platform for the exchange of information, aiming to establish a network of national contact points. Setting up a network of national contact points is a mechanism similar to the one established within Eurojust. In that case it has been a great success, as states have greatly benefited from the opportunity to improve cooperation by effective communication. Such a platform of cooperation has
proven to be of great potential. However, the question that arises is whether these types of crimes could have been brought within the already existing platform of Eurojust. This could have possibly saved resources, as well as enable Member States to take advantage of channels that have proven to be fully functional.

(c) Geographical scope

i) Eurojust

In case of an agreement with a third (non-EU) state, Eurojust can provide assistance in cases between a EU Member State and the third state. Even if such an agreement does not exist, Eurojust can still assist in specific circumstances in which there is an urgent need to provide assistance.

Cooperation in the framework of Eurojust is likely to involve several different actors and institutions. Although national members and Eurojust staff foster cooperation in criminal matters in the EU, broader cooperative relations are created by Eurojust. Eurojust and the European Judicial Network maintain privileged relations, consult and complement with each other by setting efficient cooperation mechanism. Moreover, Eurojust may establish and maintain relations with other institutions, bodies and agencies of the EU such as Europol, the European Anti-Fraud Office (OLAF), Frontex and the European Judicial Training Network. These agreements or working arrangements may concern the exchange of information as well as the secondment of liaison officers to Eurojust.

Eurojust may also establish and maintain cooperative relations with third states and conclude cooperation agreements with them or with international organisations such as Interpol. Moreover, under certain conditions, Eurojust may coordinate the execution of requests for judicial cooperation issued by a third State.

ii) Europol

Like Eurojust, Europol establishes and maintains cooperative relations with several institutions and organisations. Europol may conclude agreements or working arrangements with Eurojust, OLAF, Frontex, the European Police College (CEPOL), the European Central Bank (ECB) and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). In addition, Europol may establish cooperative relations with third States and non-European organisations such as Interpol, in so far as it is necessary for the performance of its tasks. These cooperative agreements or working arrangements may concern the exchange of operational, strategic or technical information, including the exchange of personal data and classified information.

(d) Multilingualism

Being an agency of the EU, the official linguistic arrangements of the Union apply to Eurojust proceedings. Also, the annual reports issued by Eurojust are drawn up in all the official languages of the EU. To this end, Eurojust is provided with a translation service whose budget forms part of the EU budget. Europol’s activity is carried out in all languages of the EU.

(e) Costs

Eurojust has its own budget, which forms part of the general budget of the EU. It is adopted every year by the College of Eurojust, and then submitted to the Council for endorsement and to the European Parliament for information. Eurojust expenditure includes, *inter alia*, costs relating to interpreters and translators, expenditure on security, administrative and infrastructure expenditure, operational and rental costs, travel expenses of members of Eurojust and its staff and costs arising from contracts with third parties.

Europol is endowed with its own financial resources, which form part of the general budget of the EU. Its budget is adopted by the Europol Management Board every year and is then submitted to the Council for endorsement and to the European Parliament for information. Europol’s expenditure includes its staff, administrative, infrastructure and operational expenses. The Europol Convention clarifies that “the costs incurred by national units in communications with Europol shall be borne by the Member States and, apart from the costs of connection, shall not be charged to Europol”.

(ff) Use of technology

The exchange of information in the framework of Eurojust is significantly enhanced thanks to the Eurojust Case Management System. This instrument is intended mainly to support the management and coordination of investigations and prosecutions for which Eurojust is providing assistance and to facilitate
access to information on those cases. Likewise, each national member should keep temporary work files for every case with respect to which information is transmitted to him, including information on terroristic offences. Each national correspondent who has opened a temporary work file shall decide on a case-by-case basis “whether to keep the temporary work file restricted or to give access to it or to parts of it to other national members or to authorised Eurojust staff”.

A sophisticated information processing system allows Europol and national units to exchange information and intelligence among each other. Europol maintains the Europol Information System, which, to a certain extent, can be considered as the European police database. This system is employed only to process information that is necessary for the performance of Europol’s tasks and contains data on persons who are suspected of having committed a crime, have taken part in a criminal offence or have been convicted of such offences. It further contains data on persons “regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences” in the future. Data in the Europol Information System can be entered and retrieved by national units, liaison officers and duly empowered Europol staff.

Similarly, Europol is competent to establish and maintain analysis work files concerning certain criminal offences. Europol may store, modify or use data on offences in analysis work files where this is necessary for the performance if its tasks. Moreover, an index function is created by Europol for the data stored in the analysis work files. The index function facilitates the consultation of those data by authorities who can have access to it, that is duly empowered Europol staff, liaison officers and members of the national units.

(g) Time

Shortening time limits in criminal justice cooperation is of the utmost importance. Such an achievement may be realized not only by the use of technologies, but also by prescribed time-frames for action and contact points available 24/7.


**Article 17**

**Time limits and procedures for the decision to execute the European arrest warrant**

1. A European arrest warrant shall be dealt with and executed as a matter of urgency.
2. In cases where the requested person consents to his surrender, the final decision on the execution of the European arrest warrant should be taken within a period of 10 days after consent has been given.
3. In other cases, the final decision on the execution of the European arrest warrant should be taken within a period of 60 days after the arrest of the requested person.
4. Where in specific cases the European arrest warrant cannot be executed within the time limits laid down in paragraphs 2 or 3, the executing judicial authority shall immediately inform the issuing judicial authority thereof, giving the reasons for the delay. In such case, the time limits may be extended by a further 30 days.
5. As long as the executing judicial authority has not taken a final decision on the European arrest warrant, it shall ensure that the material conditions necessary for effective surrender of the person remain fulfilled.
6. Reasons must be given for any refusal to execute a European arrest warrant.
7. Where in exceptional circumstances a Member State cannot observe the time limits provided for in this Article, it shall inform Eurojust, giving the reasons for the delay. In addition, a Member State which has experienced repeated delays on the part of another Member State in the execution of European arrest warrants shall inform the Council with a view to evaluating the implementation of this Framework Decision at Member State level.

Furthermore, from a broader perspective, the success of the EAW can largely be defined in terms of shortening the time needed for traditional extradition between EU Member States. The average time required to complete an extradition procedure has dramatically declined under the EAW. The first year in which the EAW was in effect is illustrative of this trend. The average time taken to execute a request has decreased from around a year under the old extradition procedure to on average 43 days, and 11 days in cases in which the person consents to surrender.

To deal with matters of urgency, Eurojust has established the on-call coordination (OCC). The OCC is put in place by Eurojust and relies on one representative per Member State. The OCC national contact point is able to act and can be contacted on a 24/7. The OCC can also be contacted in urgent cases when a request or decision needs to be executed in more than one Member State. In this case, the competent authority of a Member State may contact the OCC. In turn, the OCC is obliged to immediately forward the request or decision to the OCC national contact point of the Member State from which the request originates and may
also forward it to the OCC representative of the Member State which should execute the request. Thus, this procedure ensures prompt coordination among Member States on a permanent basis.
2.6  Fundamental rights (in passim)

2.6.1  Legal framework

Past

- Council Regulation (EC) No 1035/97 of 2 June 1997 establishing a European Monitoring Centre on Racism and Xenophobia\(^{134}\)

In force


2.6.2  General overview

(a)  European Union Agency for Fundamental Rights (FRA)

FRA Regulation (2007)

Article 2
Objective
The objective of the Agency shall be to provide the relevant institutions, bodies, offices and agencies of the Community and its Member States when implementing Community law with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights. […]

Article 4
Tasks
1. To meet the objective set in Article 2 and within its competences laid down in Article 3, the Agency shall:

(a) collect, record, analyse and disseminate relevant, objective, reliable and comparable information and data, including results from research and monitoring communicated to it by Member States, Union institutions as well as bodies, offices and agencies of the Community and the Union, research centres, national bodies, non-governmental organisations, third countries and international organisations and in particular by the competent bodies of the Council of Europe;
(b) develop methods and standards to improve the comparability, objectivity and reliability of data at European level, in cooperation with the Commission and the Member States;
(c) carry out, cooperate with or encourage scientific research and surveys, preparatory studies and feasibility studies, including, where appropriate and compatible with its priorities and its annual work programme, at the request of the European Parliament, the Council or the Commission;
(d) formulate and publish conclusions and opinions on specific thematic topics, for the Union institutions and the Member States when implementing Community law, either on its own initiative or at the request of the European Parliament, the Council or the Commission;

\(^{134}\) OJ L 151, 10.06.1997, pp. 1–7.
(e) publish an annual report on fundamental-rights issues covered by the areas of the Agency's activity, also highlighting examples of good practice; 
(f) publish thematic reports based on its analysis, research and surveys; 
(g) publish an annual report on its activities; and 
(h) develop a communication strategy and promote dialogue with civil society, in order to raise public awareness of fundamental rights and actively disseminate information about its work. […]

**Article 6**

**Working methods**

1. In order to ensure the provision of objective, reliable and comparable information, the Agency shall, drawing on the expertise of a variety of organisations and bodies in each Member State and taking account of the need to involve national authorities in the collection of data:

(a) set up and coordinate information networks and use existing networks; 
(b) organise meetings of external experts; and 
(c) whenever necessary, set up ad hoc working parties.

2. In pursuing its activities, the Agency shall, in order to achieve complementarity and guarantee the best possible use of resources, take account, where appropriate, of information collected and of activities undertaken, in particular by:

(a) Union institutions and bodies, offices and agencies of the Community and the Union, and bodies, offices and agencies of the Member States; 
(b) the Council of Europe, by referring to the findings and activities of the Council of Europe's monitoring and control mechanisms and of the Council of Europe Commissioner for Human Rights; and 
(c) the Organisation for Security and Cooperation in Europe (OSCE), the United Nations and other international organisations.

3. The Agency may enter into contractual relations, in particular subcontracting arrangements, with other organisations, in order to accomplish any tasks which it may entrust to them. The Agency may also award grants to promote appropriate cooperation and joint ventures, in particular to national and international organisations as referred to in Articles 8 and 9. […]

**Article 8**

**Cooperation with organisations at Member State and international level**

1. In order to ensure close cooperation with Member States, each Member State shall nominate a government official as a National Liaison Officer, who shall be the main contact point for the Agency in the Member State. […]

2. To help it carry out its tasks, the Agency shall cooperate with:

(a) governmental organisations and public bodies competent in the field of fundamental rights in the Member States, including national human rights institutions; and 
(b) the Organisation for Security and Cooperation in Europe (OSCE), especially the Office for Democratic Institutions and Human Rights (ODIHR), the United Nations and other international organisations. […]

**Article 9**

**Cooperation with the Council of Europe**

In order to avoid duplication and in order to ensure complementarity and added value, the Agency shall coordinate its activities with those of the Council of Europe, particularly with regard to its Annual Work Programme pursuant to Article 12(6)(a) and cooperation with civil society in accordance with Article 10. […]

**Article 10**

**Cooperation with civil society; Fundamental Rights Platform**

1. The Agency shall closely cooperate with non-governmental organisations and with institutions of civil society, active in the field of fundamental rights including the combating of racism and xenophobia at national, European or international level. To that end, the Agency shall establish a cooperation network (Fundamental Rights Platform), composed of non-governmental organisations dealing with human rights, trade unions and employer's organisations, relevant social and professional organisations, churches, religious, philosophical and non-confessional organisations, universities and other qualified experts of European and international bodies and organisations.

2. The Fundamental Rights Platform shall constitute a mechanism for the exchange of information and pooling of knowledge. It shall ensure close cooperation between the Agency and relevant stakeholders.
3. The Fundamental Rights Platform shall be open to all interested and qualified stakeholders in accordance with paragraph 1. The Agency may address the members of the Fundamental Rights Platform in accordance with specific needs related to areas identified as a priority for the Agency’s work. […]

**Article 16**

**Independence and public interests**

1. The Agency shall fulfil its tasks in complete independence. […]

**Article 20**

**Drawing up of the budget**

[…] 3. The revenue of the Agency shall, without prejudice to other resources, comprise a subsidy from the Community, entered in the general budget of the European Union (Commission section).

The main role of FRA is to support EU policy making by advising on its compliance with fundamental rights. This way the FRA contributes to the principle of good governance, according to which the decisions are made based on informed assessments. The establishment of the Agency in 2007 forms a part of a bigger process of EU commitment to the observance of fundamental rights, which includes the enactment of the Charter of Fundamental Rights, as well as attempts to adhere to the ECHR (cf. e.g. Sokhi-Bulley 2011, 683–706; Toggenburg 2013, 1–23).


**The Agency: a glimpse at its role in the EU’s institutional landscape**

FRA is the only EU body that is solely and specifically tasked to deal with the protection of fundamental rights. In contrast to the three major EU institutions – the Council of the European Union, the European Commission and the European Parliament – FRA is not a political institution. It is an expert body that “shall fulfil its tasks in complete independence”. Moreover, FRA is not – unlike the EU institutions – entitled to issue legally binding decisions. Finally, unlike, the Court of Justice of the European Union (CJEU), the European Ombudsman or the European Parliament’s Petitions Committee, FRA is not tasked to deal with individual complaints.

The Agency has an advisory role; its objective is to provide the relevant EU institutions and other bodies of the European Union and its Member States “with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights”.

To fulfill this overall objective of providing assistance and expertise in the area of fundamental rights, the agency is entrusted with different tasks that can be clustered under three main categories:

Firstly, it collects and analyses information and data in specific thematic areas. These themes are normally those defined in its Multiannual Framework […] However, on request the agency can collect data and provide analysis on fundamental rights issues falling outside this framework but, of course, within EU competence.

Secondly, the agency uses the evidence drawn from its research to formulate advice for both the EU institutions and Member States. Such ‘evidence-based advice’ can take a variety of forms, including reports, opinions, workshops or informal input to the EU institutions.

Thirdly, the agency is tasked to raise awareness of fundamental rights and promote dialogue with civil society organisations. Again, this is done through a variety of means and formats, including online tools or the Fundamental Rights Platform. […]

What, however, can be said after five years of the agency being in place and against the backdrop of the overall fundamental rights landscape of the EU, is that the FRA adds value to the fundamental rights landscape in Europe by providing a variety of innovative elements, including:

- socio-legal research covering all EU Member States thus providing comparable information and analysis across the EU;
- focus on rights holders (individuals) as opposed to duty bearers (states), thus providing information also on the situation on the ground (rather than the law in the books);
- outreach to civil society, including through its Fundamental Rights Platform that brings together over 350 NGOs through annual meetings and online consultations;
Fundamental rights (in passim)

— role as an independent expert body within the EU, including through its legal opinions on draft EU legislation [...] ;
— a ‘joined-up governance approach’ to the protection of fundamental rights in the EU, also taking full account of the contribution of local and regional actors as well as the United Nations and the Council of Europe and developing networks with equality bodies, National Human Rights Institutions or Ombudspersons.


Structurally, the Agency operates through nodes of experts at the EU, national and international levels. At the EU level the four structural bodies of the Agency are: the Director, Management Board, Executive Board and Scientific Committee. The FRA includes networks at the national level; until 2011 these were RAXEN (groups of experts collecting data on issues concerning racism, xenophobia and related intolerances) and FRALEX (the FRA’s ‘group of legal experts’, who report on legal aspects of fundamental rights issues in all Member States). These have been merged into FRANET. The FRA’s networks extend to ‘other’ bodies, which adds an international level to the organisation of the Agency – these bodies include the UN and the Organisation for Security and Cooperation in Europe (OSCE), the Council of Europe and human rights NGOs.

The Agency’s working methods entail gathering data and information, which it releases as its ‘products’. The major products of the FRA are its annual reports, thematic reports and surveys. [...] A second major product of the Agency is the results of ‘EU-MIDIS’, the European Union Minorities and Discrimination Survey, which is the first ever EU-wide survey to record the experiences of discrimination and racist crime suffered by immigrant and ethnic minority persons resident in the EU Member States.

(b) European Network of Equality Bodies (Equinet)

Equinet is the European Network of Equality Bodies. It brings together independent organisations from 33 European countries whose task is to promote equality and counter discrimination on grounds of age, gender, disability, race, ethnic origin, religion and sexual orientation. Member States were obliged to set up national equality bodies pursuant to the Racial Equality Directive and the Gender Goods and Services Directive (as well as the Gender Recast Directive). The competences of equality bodies include providing assistance to victims of discrimination, conducting independent surveys concerning discrimination, publishing independent reports and making recommendations on any issue relating to discrimination.

Equinet’s mission consists in supporting “equality bodies to be independent and effective as valuable catalysts for more equal societies”. This aim is achieved through the exchange of information, data and expertise from and among national equality bodies, holding regular training seminars for staff members and experts within national equality bodies and establishing collaboration within ad hoc working groups on thematic work areas. (Thus far, four working groups are set up in the framework of Equinet, namely: Equality Law in Practice; Communication Strategies and Practices; Policy Formation; and Gender Related Issues.) Moreover, Equinet encourages cooperation among national equality bodies by publishing studies and reports on relevant themes and on policy developments relating to equality and non-discrimination in the EU, as well as on the work of national equality bodies.

The European Commission, DG JUST under the Rights, Equality and Citizenship Programme 2014-2020, currently funds Equinet.

(c) European Information Network on Racism and Xenophobia (RAXEN)

RAXEN is a tool which has been used by the EUMC and subsequently by the FRA to provide the European Union and Member States with objective and reliable data on the phenomena of racism, xenophobia and anti-Semitism. RAXEN is a network composed of 25 national focal points (NFPs). They are the entrance points of FRA at national level regarding the data and information collection foreseen in RAXEN. NFPs are organisations, associations and/or research bodies established at national level whose mission is to combat racism, xenophobia and anti-Semitism and to collect information, data and statistics on these phenomena. NFPs transfer data of this kind to FRA, which coordinates them.

European Network Against Racism (ENAR)

European Network Against Racism (ENAR), gathers European NGOs working against racism in all EU Member States. Established in 1998, ENAR promotes the exchange of information among Member States on EU policy developments and their anti-racism legislation, the exchange of experiences and know-how and the development of common strategies at EU level to tackle this problem. ENAR cooperates with European and international organisations to this end, such as FRA, the Council of Europe and the UN Committee on the elimination of racial discrimination.

2.6.3 Observations

We have had a brief look at the cooperation in the field of fundamental right protection in the EU as it builds predominantly of gathering and analysing information with a view to support policy making. It gathers this information from a variety of stakeholders, both from inside the EU as well as from outside, and it does so in informal yet structured way. The example of FRA suggests that formal cooperation, e.g. concerning enforcement, should be supplemented by informal one, e.g. concerning precisely evidence gathering to support policy-making.

In the recent years FRA has produced significant analysis concerning data privacy law, and among others an opinion on the proposed data protection reform package (2012),\textsuperscript{141} a study on access to remedies (2014)\textsuperscript{142} and a handbook on European data protection law (2014).\textsuperscript{143} It is currently occupied with fundamental rights implications of biometric data in large EU IT systems in the areas of borders, visa and asylum (2014 onwards).\textsuperscript{144}

We do not opt for an establishment of a “EU Institute for Personal Data Protection” but we suggest that FRA (and perhaps similar actors) should take much more active role in a debate on data protection. This comes with a need for additional resources (time, money, manpower) as well as organisational change within the FRA.

### Matrix

<table>
<thead>
<tr>
<th></th>
<th>Migration and border control</th>
<th>Private international law</th>
<th>Consumer protection</th>
<th>Competition law</th>
<th>Criminal justice</th>
<th>Fundamental rights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Mutual trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Legality</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>National differences</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Extraterritoriality</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Geographical scope</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Gradual development</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>Multilingualism</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>Costs</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>9</strong></td>
<td>Use of technology</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>10</strong></td>
<td>Coordinated enforcement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>11</strong></td>
<td>ADR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>12</strong></td>
<td>Time</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>13</strong></td>
<td>Formal &amp; informal cooperation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**main occurrence in the area of cooperation**

**example**

- Brussels I Reg. (recast) Recital 26
  - firm legal basis
  - legally binding (obligatory enforcement)
  - comprehensive (incl. procedures)

- grounds for refusal [EIO Dir. Art 11] (e.g. ordre public)

- CISA Art 40
  - *exequatur*
  - Eurojust ■ Europol

- CIS Reg. Art 19
  - FRA Reg. Arts 8-10

- *exequatur*
  - revision clauses [CPC Reg. Art 21a]

- exchange of alphanumeric information
  - ‘alphanumeric certificates’
  - prior agreement as to use of languages
  - consumer: her own language
  - *EU agencies/bodies*: all official languages

- ‘own share principle’
  - *EU agencies/bodies*: EU budget
  - specific EU funding [EEC-Net; Dec. 1926/2006]

- SIS II ■ N.SIS II ■ VIS ■ Eurodac ■ EU-Lisa ■ CIS
  - CPC System ■ ECC-Net case handling database
  - ECN
  - Eurojust Case Management System
  - Europol Information System

- CPC Reg. Art 9 (‘sweeps’)

- ADR Dir.
  - ODR Reg. ■ ODR Platform

- single liaison officer (SLO) ■ national contact points (NCP)
  - Eurojust On-Call Coordination (OCC)

- Eurojust
  - FRA

---

145 Text in *blue* refers to a particular legal provision.
4 Conclusions


1. The quest for efficient cooperation in data privacy law

There is a critical need to improve the functioning of cross-border cooperation of supervisory authorities in the area of data privacy law (hereinafter: cooperation). Privacy violations in the present-day globalised and digitalised world often do not stop at the borders of a single jurisdiction. Consequently, these authorities more often need to work together closely; both to sanction such violations, should they occur and to develop policies and practices to minimise the risk of such violations occurring.

This necessity to improve the functioning of such cooperation has to do with its contemporary inefficiency. Nowadays cooperation faces numerous barriers and obstacles, 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. Building on the analysis of these impediments, in our previous works (Kloza and Galetta 2015) we have argued for efficient cooperation – i.e. «functioning or producing effectively and with the least waste of effort» – as in many Western liberal democracies there are fundamental rights at stake. And these rights need to enjoy «practical and effective» protection, to which efficient cooperation contributes.

We have subsequently offered recommendations for improving its efficiency and one of them was to look comparatively at parallel cooperation mechanisms as these might prove instructive. We have observed there exist other cooperation mechanisms that – having had faced similar barriers and obstacles much earlier – have eventually reached relative maturity, efficiency and success (Kloza and Mościbroda 2014). Tasked by a European research project, we have therefore looked at numerous cooperation mechanisms in the laws and policies of the EU in order to identify best practices from these that could possibly be adapted to the needs and reality of EU data privacy law.

This exercise has resulted in the selection of twelve lessons drawn from areas ranging from border control to competition law and consumer protection to private international law and criminal law. Yet here we have not sought to be exhaustive. The said variety is an outcome of our selective reading of legal instruments and academic literature and of subsequent «cherry picking» those elements that we would find simply useful for improving the efficiency of cooperation.

[…]

2. Existential lessons

1. Cooperation should be based on the presumption of the equal value, competence and standing of each supervisory authority and of the legal system in its jurisdiction and thus on the principle of mutual trust.

We have observed that mutual trust in the administration of justice in the Member States is pivotal to the functioning of EU private international law (PIL). As early as 1968, such trust has enabled automatic recognition of judgments given in other Member States «without any special procedure being required». Some 40 years later, in 2012, it has further justified the abolition of the exequeratur (i.e. declaration of enforceability), thus bringing the EU PIL closer to the ideal of the Full Faith and Credit Clause in the American Constitution.

2. Cooperation should be firmly based in law, at least when supervisory authorities enforce data privacy laws.

Collective reading of all legal instruments analysed for the present exercise has revealed that each cooperation mechanism is based on a binding and comprehensive legal instrument, most often a regulation. In the areas of consumer protection and competition law, even a dedicated regulation has been enacted to that end.

3. Cooperation should respect national and regional differences of the jurisdictions involved.

We agree with De Hert and Willems (2015) that cooperation in the area of criminal justice is often an

\textsuperscript{146} Original footnotes omitted.
expression of differences between national legal systems and cultures. Some jurisdictions will not give up control over aspects that they regard as fundamental and only by allowing exceptions – e.g. grounds for refusal – cooperation, and especially such sensitive aspect thereof as enforcement – would ever be possible.

4. **Supervisory authorities should be able to exercise – to a reasonable extent – extraterritorial jurisdiction.**

Following Svantesson (2013), we have made this argument in our earlier works, but now our comparative exercise has confirmed our conviction. Perhaps the most pertinent example of extraterritorial jurisdiction is the Schengen system. If a person is presumed to have taken part in an extraditable criminal offence and he has moved from one Schengen state to another, the former state can keep conducting investigations on him «on the ground» and beyond its national borders, as long as authorised by the latter. Furthermore, for a number of violent and serious crimes, in a situation of urgency, such an authorisation is initially replaced by mere notification.

5. **Cooperation should have as broad geographical scope as possible.**

There exist cooperation mechanisms that explicitly permit and oblige authorities to cooperate with their counterparts from third states and with international organisations, often offering an elaborated framework therefor. We see it as an acknowledgment that – due to the nature of objects these mechanisms seek to protect – it makes little sense to limit their protection solely to the EU borders. For example, «Eurojust may establish and maintain cooperative relations with […] third States [and] organisations such as […] the International Criminal Police Organisation (Interpol)». Due to the nature of the European single market, the consumer protection cooperation extends to Norway and Iceland.

6. **Cooperation should be developed gradually and its functioning should be reviewed periodically.**

Many of these cooperation mechanisms have been introduced step-by-step, thus acknowledging their experimental nature. The development of EU PIL looks like a stepping stone rather than a stumbling block. The early areas to harmonise were selected very carefully and such harmonisation was first achieved in 1968 by a means of an international treaty under the auspices of then-European Economic Community. The most controversial element – the exequatur in civil matters – has been gradually abolished from 2004: first for the uncontested claims and only in 2012 for all civil matters. In parallel, many of the instruments analysed contain some form of a revision clause, be it the need for an external review or simply a report on the functioning of the instrument.

3. **Practical lessons**

7. **The need for translation and interpretation should be reduced to absolute minimum. The type of information exchanged should determine the very need for translation and interpretation. Supervisory authorities should have a right to waive such a need. Supranational legal provisions should govern the linguistic regime.**

We have first observed the problem of multilingualism in cooperation is not of a uniform nature. In some instances, for example in border protection databases, the use of multiple languages is not likely to pose any barriers as the information exchanged consist merely of alphanumeric data, e.g. names or car plates. Similarly, the EU PIL works on standardised certificates, which might require translation in exceptional situations. In other instances, when the need to share some documentation occurs, the problem of its translation might arise. (We said «might» as we do not expect the need for translation of a document issued by an authority in e.g. Salzburg intended to be sent to a counterpart authority in e.g. Munich.) In customs cooperation, a request for assistance should be accompanied by translation to a language of the state being asked, but this state can waive this requirement. In consumer protection cooperation, «the languages used […] shall be agreed […] before requests have been made». If no agreement can be reached, each jurisdiction uses its own language. What links these diverse solutions is the governance of the linguistic regime on a supranational level.

8. **Stakeholders should share the costs of cooperation.**

As there are various solutions for dealing with multilingual nature of the EU, so there are different solutions for sharing the costs of cooperation. For example, in border control databases, due to their technical design, the costs of running national units are borne by the Member States concerned, while the general EU budget covers the costs of the central unit of each database. Conversely, in consumer protection cooperation «all claims for the reimbursement of expenses incurred» shall normally be waived.

9. **Cooperation should maximise the use of information and communication technologies.**

The majority of cooperation mechanisms analysed relies on sharing information. And such sharing occurs with the help of technology. Well known examples are border control databases, but consumer protection and competition law cooperation too have their own platforms for sharing relevant case-related
Conclusions

The above-mentioned 12 lessons have been discussed at the Internationales Rechtsinformatik Symposium (IRIS 2016; Salzburg, Austria, 25-27 February) conference and subsequently presented to the PHAEDRA Advisory Board, thus permitting supplementing them by the following:

10. *Cooperation should pay equal attention to the development of policies and practices preventing data privacy violations from occurring.*

In the majority of cooperation mechanisms analysed, due to their nature, much attention is paid to ex post cooperation. However, the ex ante counterpart is often neglected. The European Consumers Centres Network (ECC-Net) is perhaps a standalone example of a mechanism explicitly tasked with coordinated «surveillance and enforcement actions» (sweeps), i.e. sets of checks carried out simultaneously by competent authorities to identify breaches of relevant laws in a given sector.

11. *Supervisory authorities should support alternative dispute resolution (ADR) methods for data subjects and controllers/processors, this including ADR by electronic means.*

Out-of-court dispute resolution is usually easier, faster and cheaper. From 2016 Europeans will enjoy a possibility to solve their consumer disputes regarding a product or service they bought using an on-line platform. We see no reason to exclude cross-border disputes between data subjects and controllers/processors from using such possibilities.

12. *Supervisory authorities should be both empowered and obliged to act speedily on cross-border data privacy violations.*

Time is of essence, especially in a digitalised and globalised world. In the cooperation toolbox, we have found a number of impeccable tools for urgent reaction to violations of relevant laws. Many instances provide for single liaison officers and Europol, for instance, has launched the On-Call Coordination (OCC) mechanism.

The above-mentioned 12 lessons have been discussed at the Internationales Rechtsinformatik Symposium (IRIS 2016; Salzburg, Austria, 25-27 February) conference and subsequently presented to the PHAEDRA Advisory Board, thus permitting supplementing them by the following:

13. *Informal mechanisms for cooperation shall supplement the formal ones.*

The spectre of cross-border cooperation activities varies significantly from “soft” ones, such as ex ante public awareness raising, to “hard” ones, such as ex post enforcement of laws. The challenging goal of efficiency should not be reached by using “hard” forms of cooperation only. 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 (cf. Baggaley 2014; Kloza and Galetta 2015).


The critical need to improve the functioning of cross-border cooperation of supervisory authorities in the area of data privacy law has been already articulated on a numerous occasions. The late Ulrich Beck (1944-2015), a German sociologist who explored the theme of global risks in the modern interconnected world, argued that "world risk society brings a new, historic key logic to the fore: No nation can cope with its problems alone" (Beck 2007, 288). Global risks transcending national borders, such as terrorism, have indeed triggered global responses, which, in turn, have given rise to more global risks for long-established rights, such as privacy.

Beck does not speak about privacy, but his analysis nevertheless applies. Privacy violations in the present-day globalised and digitalised world often do not stop at the borders of a single jurisdiction. Therefore, supervisory authorities need to re-evaluate their role in light of this new world order and embrace the call for effective transnational cooperation. Consequently, these authorities more often need to work together closely: both to sanction such violations, should they occur and to develop policies and practices to minimise the risk of such violations occurring. Beck calls for an approach of transnationalization (Beck 2002, 53). National states and their authorities cannot any longer by themselves guarantee rights and freedoms recognized in their domestic legal system. Sharing a bit of their sovereignty is the way forward and paradoxically a better way of fulfilling this constitutional role of protecting rights and freedoms of their citizen.

147 Cf. https://www.univie.ac.at/RI/IRIS16.
5 Bibliography


Bibliography


