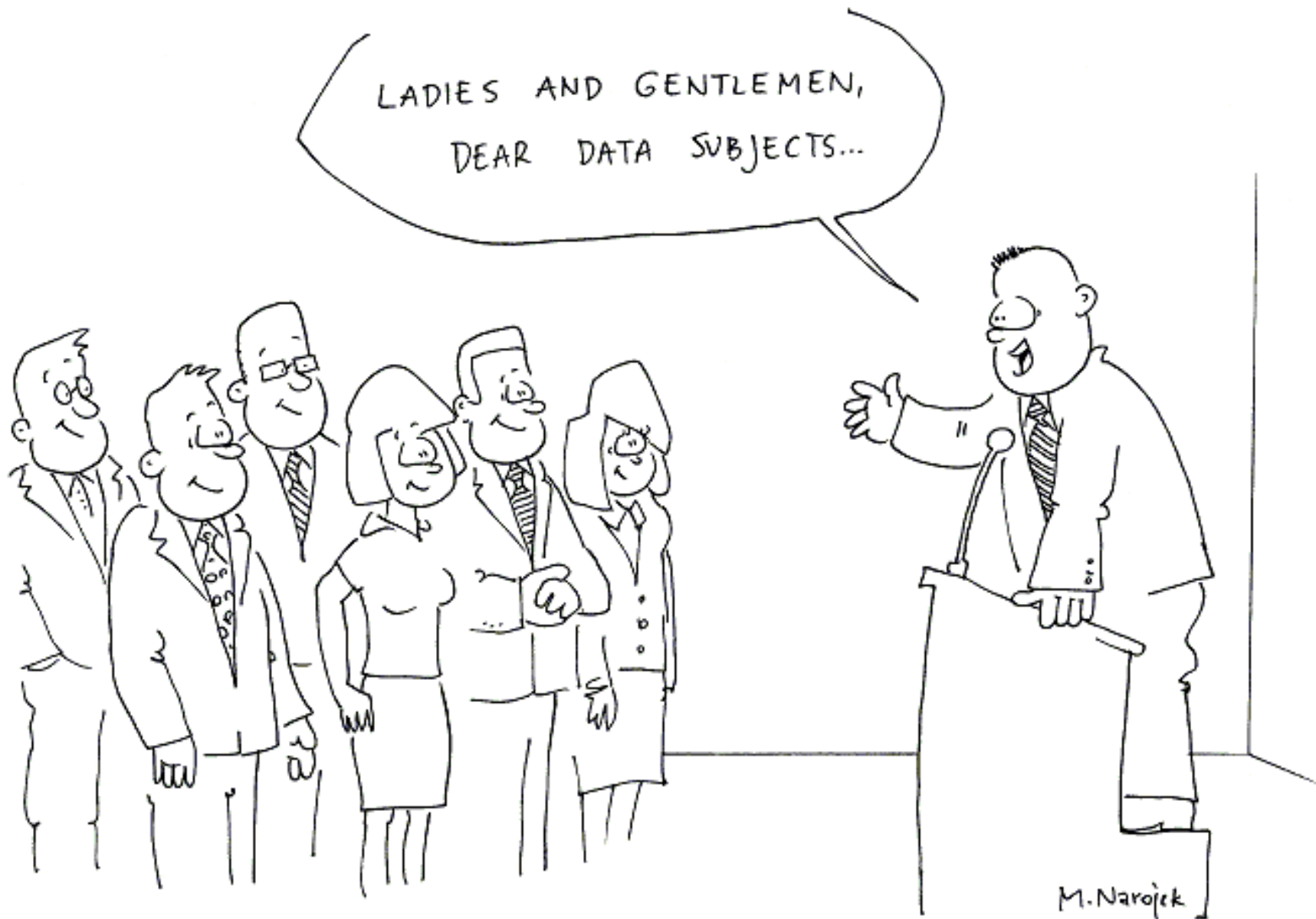




International Cooperation. Personal Data Protection Agreements and Enforcement cooperation

Wojciech Wiewiórowski
European Data Protection Assistant
Supervisor

46th APPA Forum
Asia Pacific Privacy Authorities
Manzanilla, Mexico, 30 Nov.-2 Dec. 2016



EDPS



The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. A number of specific duties of the EDPS are laid down in Regulation 45/2001. The three main fields of work are

- **Supervisory tasks**
- **Consultative tasks:** to advise EU legislator on proposals for new legislation as well as on implementing measures. Technical advances, notably in the IT sector, with an impact on data protection are monitored.
- **Cooperative tasks:** involving work in close collaboration with national data protection authorities (Article 29 Working Party)

The role of European Data Protection Supervisor

- The **European Data Protection Supervisor (EDPS)** is the independent supervisory authority for the processing of personal data by the EU administration;
- **Privacy and data protection are fundamental rights** – see Articles 7 and 8 of the Charter of Fundamental Rights;
- **Independent supervision** is an integral part of the right to data protection – see Article 16(2) TFEU and 8(3) Charter;
- What we do:
 - monitoring and verifying compliance with Regulation (EC) 45/2001,
 - giving advice to controllers,
 - advising the co-legislators on new legislation,
 - cooperating with Member States' DPAs,
 - handling complaints, conducting inspections
 - Monitoring technological developments
 - Promoting data protection aware design and development



Who we want to be



- Active Partner for EU institutions
 - Provide practical and dynamic solutions;
 - Cooperate with DPOs, DPCs and Controllers;
 - Offer Guidance;
 - Increase interactions with EU Institutions and bodies;
 - Develop our own knowledge of EU reality so our advice is relevant.
- Selective
 - Apply selectiveness in each activity using a risk based approach so we can handle our day to day work effectively.
- Be accountable and promote accountability





Our objectives

- I. Data protection goes digital
- II. Forging global partnerships
- III. Opening a new chapter for EU data protection

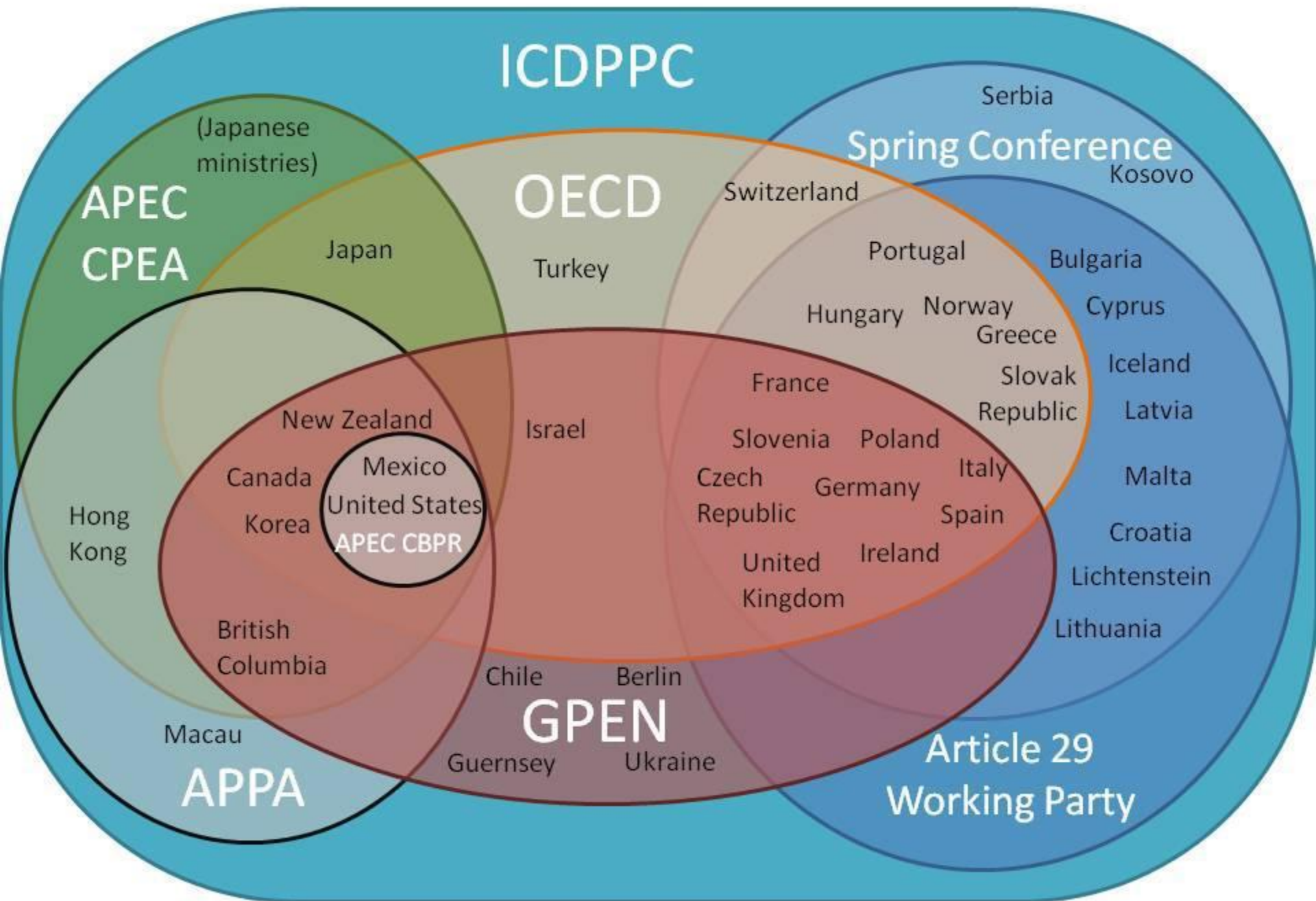


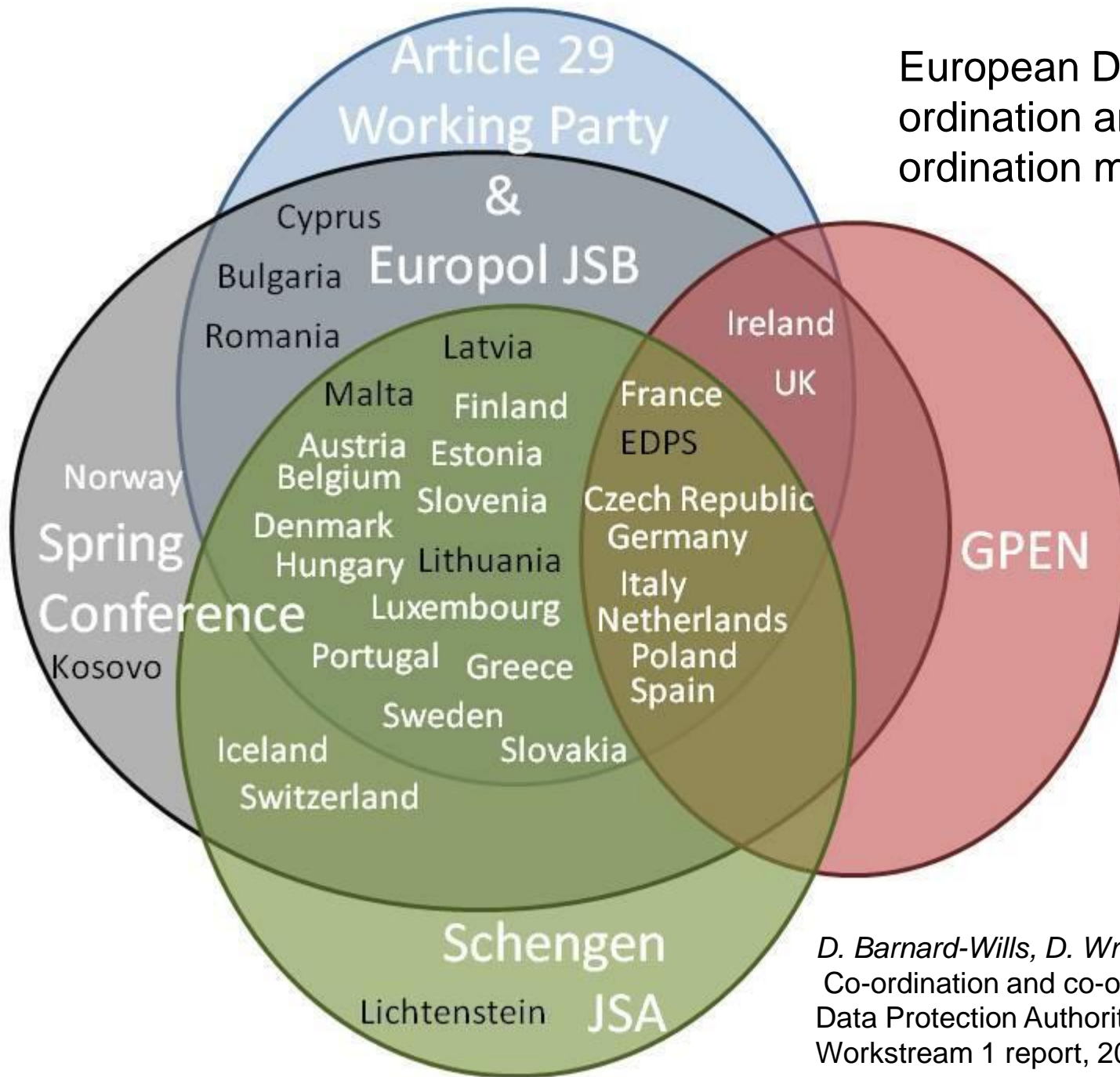
On regional co-operation in Europe



41st APPA Forum – Seoul 2014







European DPA co-ordination and co-ordination mechanisms

D. Barnard-Wills, D. Wright [ed.]
Co-ordination and co-operation between
Data Protection Authorities. Phaedra
Workstream 1 report, 2014, p. 102

International co-operation of data protection authorities (DPAs)

The International Conference of Data Protection and Privacy Commissioners has been meeting annually since the Conference was established in 1979. The purposes of the conference are:

To promote and enhance internationally personal data protection and convenes once a year. In the last few years, the Conference has grown into a one-week event, encompassing an Open Session accessible to all professionals involved in privacy rights.

To draft and adopt joint resolutions

To be a meeting point between accredited members and other international fora or organisations that share common objectives.

To encourage and facilitate cooperation and the exchange of information among accredited members, in particular regarding enforcement actions.

To promote the development of international standards in the field of protection of personal data.

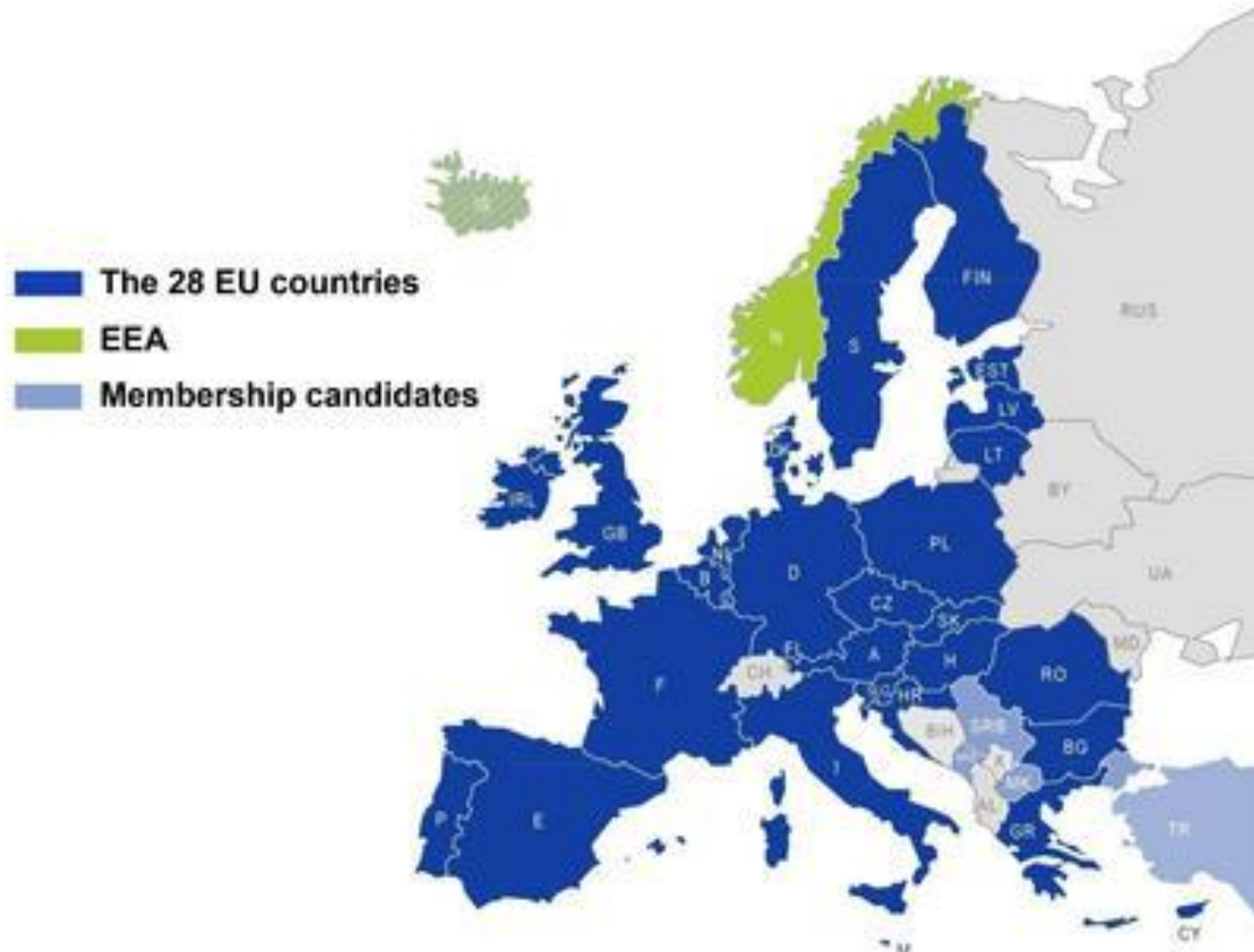


European co-operation of data protection authorities (DPAs)

- The data protection authorities from Member States of the EU and of the Council of Europe meet annually for **the European Conference of Data Protection Commissioners** (also known as the “**Spring Conference**”) to discuss matters of common interest and to exchange information and experiences on different topics. The European Data Protection Supervisor also actively contributes to the discussions. The one and half- to two-day conference usually ends with the adoption of a number of important documents. There is a **Case-Handling Workshop organised** under auspices of the Spring Conference



European co-operation of data protection authorities (DPAs)





International co-operation of data protection authorities (DPAs)

The Council of Europe Consultative Committee on the protection of personal data (the T-PD, which stands for *traité protection de données*) acts as a forum for exchanges on privacy challenges and developments. It was established in Chapter V of the Council of Europe Convention 108 on the protection of personal data.



The Article 29 Working Party

- The Working Party was set up under Article 29 of Directive 95/46/EC and its tasks are to (Art. 30.1):
 - (a) examine any question covering the application of the national measures adopted under the Directive in order to contribute to the uniform application of such measures;
 - (b) give the Commission an opinion on the level of protection in the Community and in third countries;
 - (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;
 - (d) give an opinion on codes of conduct drawn up at Community level.
- These tasks also apply with regard to the electronic communications sector (Art. 15.3 of Directive 2002/58/EC).

The Article 29 Working Party

The Article 29 Working Party was set up under Directive 95/46/EC and is composed of the representatives of the supervisory authorities of EU Member States, the supervisory authorities set up within the EU institutions and bodies, and a representative of the European Commission.

- Technology Subgroup
- Borders Travel Law Enforcement Subgroup,
- SG Future of Privacy,
- SG Key Provisions,
- SG E-Government,
- SG International Transfers,
- SG Financial Matters
- Co-operation Subgroup
- WADA Subgroup



The Article 29 Working Party

Role of EDPS in WP29:

- As a data protection authority (DPA), EDPS plays an advisory role.
- The aim is to ensure effective coordination with partner DPAs.
- EDPS contributes to WP29 activities taking up a share of the work, comparable to the one taken up by other DPAs, within the various subgroups.
- Selective approach (added value, EU perspective), e.g.:
 - WP29 Opinion on applicable law
 - WP29 response to the cybercrime committee of the Council of Europe on the impact of data protection regarding the Budapest Convention
 - Cooperation with WP29 Chair on the future European Data Protection Board (EDPB)

From WP 29 towards EDPB

The General Data Protection Regulation and the Directive on Police and Justice will significantly change the structure and the way the WP29 works today.

Upon the adoption of this package, the WP29 will have two years to be ready to become and act as the European Data Protection Board (EDPB).

The work programme of WP29 takes into account this transitional period which will require from all subgroups the issuance of guidelines, tools and procedures to organize the future cooperation between data protection authorities guide the relevant stakeholders in the application of the new framework (e.g. controllers, processors, data subjects) and ensure consistency in its implementation.

The Working Party will continue to analyze and provide its opinion on relevant subject matters under the current Directive 95/46/EC which either have already been on the previous work programme and should be maintained or are new topics to be dealt with in the two upcoming years.

Furthermore, the Working Party will work on increasing its interaction with international data protection authorities and other organisations and stakeholders, both within the European Union and outside.

The Article 29 Working Party

Future of Privacy subgroup

Before the entry into force of Regulation, the WP29 will continue to work on the basis of the current framework. However, during this transitional phase, the WP29 will anticipate the application of the new legal framework and should prepare its new governance model. The WP29 has elaborated an action plan to do so which will be regularly revised.

The Future of Privacy subgroup will be primarily in charge of piloting, managing and monitoring action plan of WP 29 by developing the **new governance model**, organizing issuance of appropriate tools and guidelines and proposing key decisions to the WP29 in relation with the action plan.

To fulfill these tasks that will be transversal and implicate other subgroups, the Future of Privacy subgroup will ensure coordination tasks and consistency checks for a coherent implementation of the WP29 strategy regarding the new framework

The Article 29 Working Party

Key Provisions subgroup

In light of the Regulation, the subgroup will examine the need to update previous opinions (e.g. the opinions on personal data, consent, controller/processor, applicable law, purpose limitation or legitimate interests).

The Key Provisions subgroup will in addition be dealing with the interpretation of key concepts of the new legal framework (e.g. scope, definitions, general provisions, rights of the data subject, obligations of data controllers and processors, specific data processing situations).

Technology subgroup

The subgroup will continue its works together with other subgroup(s) when appropriate on the following topics: Do not Track standard, data portability, Wi-Fi location analytics and bluetooth beacons, minimum technical specifications, e-voting, electronic monitoring of employees, user friendly and privacy-compliant ways of informing and expressing consent by way of smart devices, the e-Privacy Directive, Digital Single Market, smart meters and smart grids, data protection impact assessments and data breach impact assessment.

The subgroup will consider whether previous opinions need to be updated in light of the Regulation and also deal with the new topics (e.g. certification)

The Article 29 Working Party

International Transfers subgroup

The CJEU ruling on the *Schrems vs. Facebook* case has become a crucial point on the WP29 and on the International Transfers subgroup's agenda.

In coordination with other subgroups, the International Transfers subgroup has been tasked to analyze the consequences of the ruling on transfers' tools (e.g. Standard Contractual Clauses, BCR, ad-hoc clauses, other adequacy decisions) and on derogations for transfers.

The International Transfers subgroup will also analyze and deliver an opinion on the Privacy Shield arrangement. In addition, the subgroup will examine the impact of the Regulation on existing transfers' tools and the current cooperation procedure. More generally, the subgroup will consider whether previous opinions need to be updated in light of the Regulation.

The International Transfers subgroup will continue its work on the possible «interoperability» with Convention 108 and the OECD Guidelines and on the BCR-CBPR project with APEC

The Article 29 Working Party

Borders, Travel and Law Enforcement subgroup

The subgroup will continue its work on the following topics:

- Directive Police and Justice,
- PNR
- Terrorist Finance Tracking Program, Data retention, Transatlantic Cable Interception (together with the international transfers subgroup),
- the Cybercrime Convention, the proposals following the European
- Commission's European Agenda on Security
- consequences of the CJEU judgement *Schrems vs. Facebook*, including the analysis of relevant EU and US surveillance law.

The subgroup will also analyse the following legislative proposals: the revised Smart Borders package, the proposal to adopt the EU-US Umbrella Agreement, the proposal for a European Police Record Index System, the new counter-terrorism proposals and the European agenda on migration and the Electronic Criminal Record Information System (ECRIS) for third country nationals and stateless people (TCN).

The Article 29 Working Party

E-government subgroup

The subgroup will continue its work on the following topics:

- the implementing acts for the Regulation on electronic identification and trust services for electronic transactions in the internal market (EIDAS),
- Mobile Apps used in the public sector,
- the cloud services for e-Government services,
- the Research and Education network Code of conduct,
- the online publication of personal data of government officials,
- the E-Voting,
- the Digital Single Market Strategy for Europe.

The subgroup will work on the topic linked to E-health network.

The Article 29 Working Party

Financial matters subgroup

The subgroup will continue its work on the following topics: automatic exchange of data for tax purposes, OECD Common Reporting Standards, FATCA, the implications on data protection of International Organisation of Securities Commissions and Multilateral Memorandum of Understanding concerning consultation and cooperation and the exchange of Information, and the implications on data protection of Directive 2014/65/EU (so-called "MIFID 2") and Regulation (EU) 600/2014 (so-called "MAR").

The subgroup will also analyse the following topics: Account aggregators, the vast use by banks of data related to their clients for commercial profiling and the draft Regulation of the European Central Bank concerning the collection of granular credit and credit risk.

Cooperation subgroup

The subgroup will organise workshops on practical issues and tools of common interest, continue its work on the improvement of the WP29 website, on the follow up of the preparations of the International Conference and of the Spring Conference (focus on the question of enforcement cooperation).

It will elaborate a data protection vocabulary, examine the list of activities of the DPAs. The subgroup will also be involved in the analysis of the consequences of the CJEU judgement *Schrems vs. Facebook*, including on coordinated actions to handle complaints and to organise enforcement operations if needed.

Finally the subgroup will work on common tools and standard forms to implement the Regulation in a consistent manner (e.g. templates for designating a lead DPA, complaints forms)

All European enforcement co-operation

- WP29's impressive outcomes since early creation regarding common interpretation of EU Directive and advice to legislators
- As regards enforcement cooperation, until very recently only ad-hoc cooperation. Mention recent cases of more coordinated action.
- Why has been enforcement cooperation slower?
 - sovereignty of the state and its institutions,
 - competence of authorities,
 - question of judicial redress.

Co-ordinated supervision in European Union

Coordinated supervision with DPAs of **large scale IT systems**, currently:

- Eurodac
- Visa Information System ('VIS')
- Schengen Information System ('SIS II')
- Customs Information System ('CIS')
- Internal Market Information System ('IMI').

Activities include *inter alia* joint inspections and inquiries and work on a shared methodology;

The Secretariat of those groups is provided by the EDPS.

Co-ordinated supervision in European Union

- What is it? A platform where EDPS cooperates with DPAs to ensure effective supervision on large IT systems
- EDPS has a dual role: Secretariat and Member under Chinese walls rules.
- Now there are five Groups
 - *Eurodac, Visa (VIS), Schengen (SIS II), Internal Market Information System Customs Information System*
- We publish the results of our work after each meeting:
<https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/SupervisionCoordination>
- More to come: *Europol (2017), Smart Borders (2019), EPPO (?)*

Co-ordinated supervision Schengen Information System II

- EDPS supervises **eu-LISA** (= operational management of the **central unit of SIS II**); DPAs in Member States supervise national units & transmission to central unit;
- EDPS shall ensure that an **audit** of the SIS II central unit is conducted at the least every four years (last: 2015);
- **SCHEVAL** (= Schengen evaluation) missions (peer review by DPAs, coordinated by COM): EDPS participates as **observer**;
- DPAs are 28 EU Member States, with Ireland & Croatia as observers. Additionally, Iceland, Liechtenstein, Norway & Switzerland (= participants in SIS II).

Co-ordinated supervision Visa Information System

- EDPS supervises **central unit of the VIS** since operational in 10/2011; DPAs supervise processing by the national authorities & transmission to central unit;
- EDPS shall ensure that an **audit** of the VIS is conducted at the least every four years (last: 2015);
- Coordinated supervision: **Meetings EDPS with DPAs twice a year**;
- DPAs are 28 EU Member States, with Ireland & UK as observers. Additionally: Iceland, Liechtenstein, Norway & Switzerland (= participants in VIS).

Co-ordinated supervision EURODAC

- EDPS supervises **central unit of Eurodac** since 2004; DPAs supervise processing by the national authorities & transmission to central unit;
- According to the Eurodac Regulation, the EDPS shall ensure that an **audit** of Eurodac is conducted at the least every four years (last: 2012);
- Coordinated supervision: **Meetings EDPS with DPAs twice a year;**
- DPAs are 28 EU Member States + Iceland, Liechtenstein, Norway and Switzerland.

Other EU large scale databases

- **CIS** - The Customs Information System ('CIS') - exchange of information on customs investigations and to request other customs authorities to take specific actions. The former first pillar part of the CIS has a SCG similar to the one for SIS II, while the former third pillar part still has a Joint Supervisory Authority (JSA). There is at least one annual meeting between the EDPS and the CIS JSA. There are no periodic inspection obligations for the CIS. The Commission is controller for CIS, which is run by OLAF, which not only hosts the system, but also has read access to it.
- **FIDE** - The Customs Files Identification Database (FIDE) is an index of customs investigations in the different Member States. Legally speaking FIDE is part of CIS.
- **REX** - The Registered Exporters System (REX) will be a database of registered exporters in third countries that qualify for preferential customs treatment. The legal bases - amendments introduced in the Customs Code by Commission Implementing Regulation (EU) 2015/428. Unlike for most of the other systems, there is no obligation for the EDPS to regularly organise meetings. In fact, the legal base for REX does not formally set up a SCG, but simply states that national DPAs and the EDPS shall work together, using similar wording as for SIS II (see Article 69c(8)).

EDPS as the supervisor of central systems

Consultations

EDPS shall, either on its own initiative or on request "advise all [Union] institutions and bodies [...] on all matters concerning the processing of personal data".

Inspections

Regular inspection obligations in three of the systems. For SIS and VIS, it has to be ensured that an audit is carried out at least every four years, while for Eurodac, the obligation will be to have at least one audit every three years, starting from 20/07/15.

The EDPS will ensure that these audits happen by conducting them itself. In practical terms, this will result in inspections at eu-LISA (as management authority for SIS, VIS and Eurodac) almost every year, without prejudice to possible additional unplanned inspections. Inspections of one system may be combined with follow-up visits for systems that have been inspected before.

Complaints

The actual use and filling of the systems is done by and under the responsibility of Member States. The EDPS is thus e.g. not competent to examine whether an alert of a specific person in the SIS is justified. This is a question for national DPAs and courts.

When receiving complaints for which it is not competent, the EDPS will refer the complainants to the relevant national authorities and supervisory authorities. Where it is not clear where to refer to, the designated EDPS member of the SCGs will liaise on working level with the relevant other members of the SCGs, taking confidentiality issues into account.

EDPS as the supervisor of central systems

Prior Checks

IT systems with coordinated supervision do not necessarily fall under Article 27 of the Regulation.

Enforcement Measures

Where any of the supervision activities explained in this chapter require using enforcement measures, such as ordering rectification or imposing a ban, the EDPS will use its powers in accordance with its Policy

International co-operation of data protection authorities (DPAs)

- **The International Working Group on Data Protection in Telecommunications** has been called the **Berlin Group**, as it has been chaired by the Berlin Data Protection and Freedom of Information Commissioner since its creation in 1983. The Group is composed of experts in communication and information technologies and in personal data protection. It was formed on the initiative of national data protection authorities, under the framework of the International Conference of Data Protection and Privacy Commissioners, but its membership is not restricted to data protection authorities, also including representatives of private sector and NGO organisations. Secretariat services and a web page for the group are provided by the data protection authority of Berlin. Since the mid-1990s its work has focused upon data protection and privacy matters on the Internet. The IWGDPT meets biannually.



International co-operation of data protection authorities (DPAs)



The first **Meeting of Central and Eastern European Data Protection Commissioners** took place in Warsaw on 17 December 2001. Since then, the group has met 17 times.

This year meeting was organised in Durres (Albania) in May.

International co-operation of data protection authorities (DPAs)

- The first **Balkan Conference of personal data protection authorities** was held on 17-18 December 2012 in Skopje by the Directorate for Personal Data Protection, Republic of Macedonia in co-operation with TAIEX (the Technical Assistance and Information Exchange instrument managed by the Directorate-General Enlargement of the European Commission). The conference resulted from the meeting of personal data protection regulatory authorities as part of the Conference on the Modernization of EU legislation on the protection of personal data, also held by the Directorate, in May 2012.
- **Nordic data manager meeting** - *fællesnordiske datachefmøde*
- **Nordic caseworker meeting** - *årlige fællesnordiske sagsbehandlermøde for sagsbehandlere – fortrinsvis jurister – fra de nordiske datatilsynsmyndigheder: annual joint for practitioners - mostly lawyers - from the Nordic Data Protection Authorities*
- **Nordic technician meeting** - *Nordisk Teknikermøde*

International co-operation of data protection authorities (DPAs)

The Working Party on Information Security and Privacy (WPISP) is part of the **Organisation for Economic Co-operation and Development (OECD)** Directorate for Science, Technology and Industry. It reports to the Committee for Information, Computers and Communications Policy (ICCP), which in turn reports to the OECD Council.



International co-operation of data protection authorities (DPAs)

The origins of the **Global Privacy Enforcement Network (GPEN)** came out of the OECD work on cross-border co-operation in 2006. The OECD secretariat sent a questionnaire to OECD members on how OECD members enforce privacy, which led to a high-level, non-binding Council Recommendation. One of the items in the Recommendation concerned establishment of GPEN-like mechanism, structured like some consumer actions. GPEN was set up by the authorities who participate in it.

Founded in September 2010, GPEN aims to facilitate cross-border co-operation in the enforcement of privacy laws. Membership in GPEN enables privacy regulators from around the world to work more closely as they address risks to the personal information of their citizens.



Global Privacy Enforcement Network

International co-operation of data protection authorities (DPAs)

The second 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.

Some 26 privacy enforcement authorities in 19 countries participated in the 2014 Sweep, which took place May 12-18. Over the course of the week, participants downloaded 1,211 popular mobile apps in a bid to assess the transparency of their privacy practices.

Participants looked at the types of permissions apps were seeking, whether those permissions exceeded what would be expected based on the apps' functionality, and most importantly, how the apps explained to consumers why they wanted the personal information and what they planned to do with it.

One key conclusion from the 2014 Sweep was that as mobile apps explode in popularity, many of them are seeking access to large amounts of personal information without adequately explaining how that information is being used. More specifically, Sweep participants noted that three quarters of apps requested permission to access users' personal information; almost 60% offered insufficient pre-installation communications; 43% of privacy communications were difficult to read on the small screen; and over 30% of apps left sweepers wondering why the app required certain permissions.



International co-operation of data protection authorities (DPAs)

In 2003, the Spanish Data Protection Authority (Agencia española de protección de datos, AEPD) founded **the Ibero-American Data Protection Network (RIPD)** as an advisory forum for national data protection efforts in Latin America.³⁹⁸ The network was established as a consequence of the agreement reached at the Ibero-American Data Protection Meeting held in La Antigua, Guatemala in 2003, attended by representatives of 14 Latin American countries.

The **Association francophone des autorités de protection des données personnelles** (AFAPDP) has an important capacity-building component.³⁹⁹ The association of authorities for personal data protection of the French-speaking countries was founded in 2007 and consists of 27 authorities for personal data protection from the 24 member states of the International Organization of the Francophone. Members of the Association are authorities for personal data protection from Albania, Andorra, Austria, Belgium, Bulgaria, Burkina Faso, Canada (federal authority, Quebec and New Brunswick), Cyprus, Croatia, Czech Republic, France, Greece, Hungary, Lithuania, Luxembourg,, Macedonia, Monaco, Poland, Romania, Senegal, Slovakia, Slovenia, Switzerland, Cape Verde and Tunisia.

International co-operation of data protection authorities (DPAs)

History of the Conference

- 38th Conference – Marrakech – Morocco (October 2016)*
- 37th Conference – Amsterdam – the Netherlands (October 2015)*
- 36th Conference – Port Louis - Mauritius (2014)*
- 35rd Conference – Warsaw – Poland (2013)*
- 34th Conference – Punta del Este – Uruguay (2012)*
- 33rd Conference – Mexico City – Mexico (2011)*
- 32nd Conference – Jerusalem – Israel (2010)*
- 31st Conference – Madrid – Spain (2009)*
- 30th Conference – Strasbourg – France (2008)*
- 29th Conference – Montreal – Canada (2007)*
- 28th Conference – London – United Kingdom (2006)*
- 27th Conference – Montreux – Switzerland (2005)*
- 26th Conference – Wroclaw – Poland (2004)*
- 25th Conference – Sydney – Australia (2003)*
- 24th Conference – Cardiff – jointly hosted by the Commissioners from Republic of Ireland, Jersey, Guernsey, Isle of Man and the United Kingdom (2002)*
- 23rd Conference – Paris – France (2001)*
- 22nd Conference – Venice – Italy (2000)*
- 21st Conference – Hong Kong (1999)*
- 20th Conference – Santiago de Compostella – Spain (1998)*



25th International Conference of
**Data Protection & Privacy
Commissioners**

10 - 12 September 2003
Sydney, Australia

International co-operation of data protection authorities (DPAs)

- 19th Conference – Brussels – Belgium (1997)
- 18th Conference – Ottawa – Canada (1996)
- 17th Conference – Copenhagen – Denmark (1995)
- 16th Conference – The Hague – The Netherlands (1994)
- 15th Conference – Manchester – United Kingdom (1993)
- 14th Conference – Sydney – Australia (1992)
- 13th Conference – Strasbourg – Council of Europe (1991)
- 12th Conference – Paris – France (1990)
- 11th Conference – Berlin – F.R.Germany (1989)
- 10th Conference – Oslo – Norway (1988)
- 9th Conference – Quebec – Canada (1987)
- 8th Conference – Lisbon – Portugal (1986)
- 7th Conference – Luxembourg (1985)
- 6th Conference – Vienna – Austria (1984)
- 5th Conference – Stockholm – Sweden (1983)
- 4th Conference – London – United Kingdom (1982)
- 3rd Conference – Paris – France (1981)
- 2nd Conference – Ottawa – Canada (1980)
- 1st Conference – Bonn – F.R.Germany (1979)



Canada

EDPS



International co-operation of data protection authorities (DPAs)

The IPEN initiative was founded in 2014. It supports the creation of engineer groups working on (re)-usable building blocks, design patterns and other tools for selected Internet use cases where privacy is at stake. IPEN invites participants from different areas such as data protection authorities, academia, open source and business development, and other individuals who are committed to the finding engineering solutions to privacy challenges. The objective of the work should be to integrate data protection and privacy into all phases of the development process, from the requirements phase to production, as it is most appropriate for the development model and the application environment.

It supports networking between engineer groups and existing initiatives for engineering privacy into the Internet. This network facilitates exchange in order to coordinate work and avoid duplication, in addition to discussing which privacy oriented use cases should be addressed with priority.

IPEN is building a repository of relevant resources, making its findings and knowledge base accessible to all participants, developers and privacy experts.

A core group takes care of collection and distribution of information, liaises with other relevant initiatives, facilitates the dialogue on engineering solutions, and organises online and offline events.



Thank you for your attention!

www.edps.europa.eu
edps@edps.europa.eu



@EU_EDPS

