EU Policy Framework on Cybersecurity and Data Protection

19/09/2017, Brussels

Wojciech R. Wiewiórowski

European Data Protection Assistant Supervisor

”Cybersecurity and Data Protection Standards in support of European policy”

European Data Protection Supervisor (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

Our objectives

I. Data protection goes digital

II. Forging global partnerships

III. Opening a new chapter for EU data protection

European fundamental right

Treaty on Functioning of European Union – Article 16

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent auhorities.
3. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

European Union

Directive 95/46/EC
on the protection of individuals
with regard to the processing of personal data
and on the free movement of such data
(*Data Protection Directive*),
OJ 1995 L 281

Reform of Data Protection Law in the European Union

Reform of Data Protection Law in the European Union

ISSN 1977-0677

Official Journal

of the European Union

L 119

English edition

Legislation

Volume 59
4 May 2016

Contents

I Legislative acts

page

Not an absolute right

(4) **The processing of personal data should be designed to serve mankind**. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

Accountability in the new legal framework

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

Art. 5 GDPR

Accountability in the new legal framework

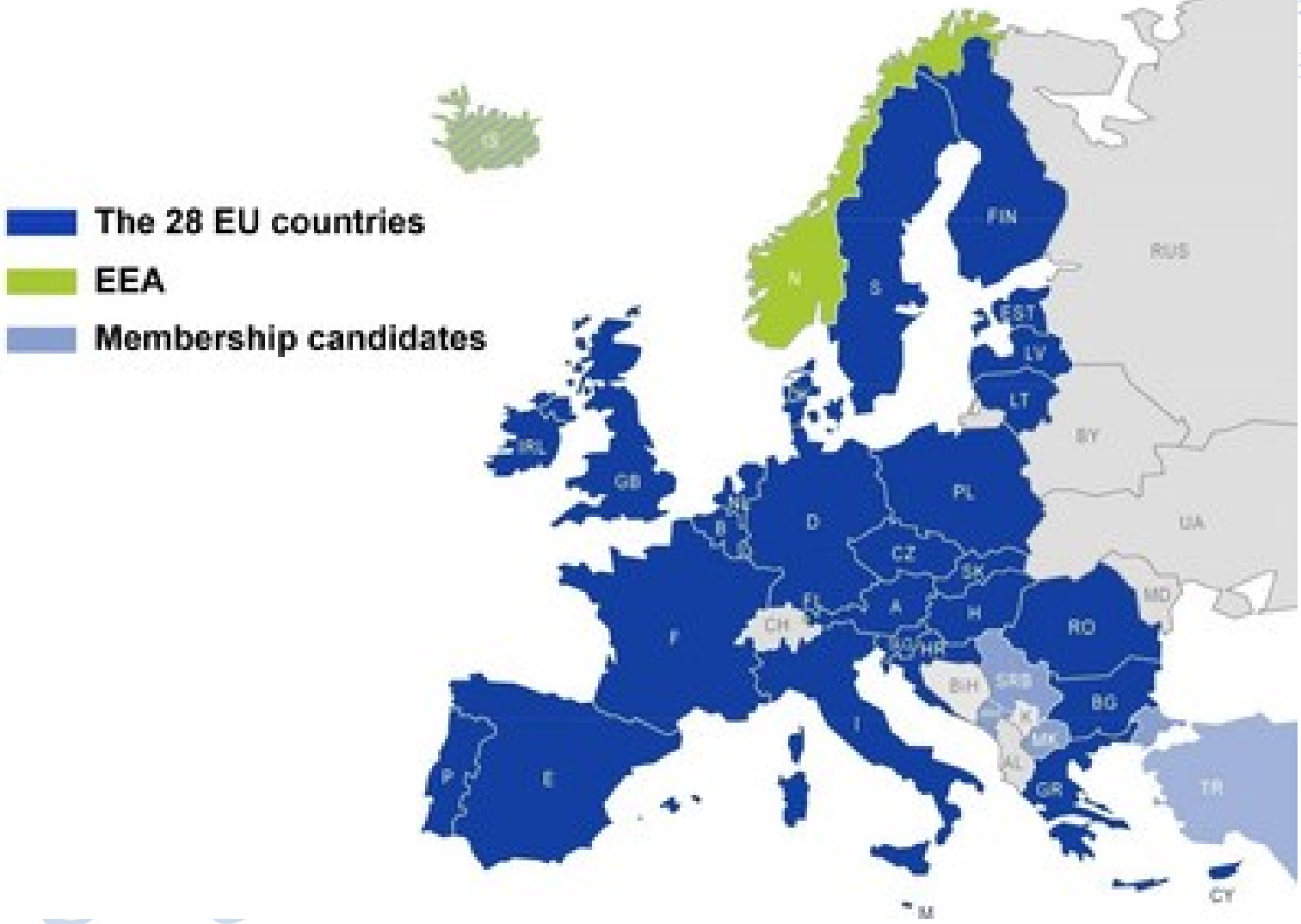
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

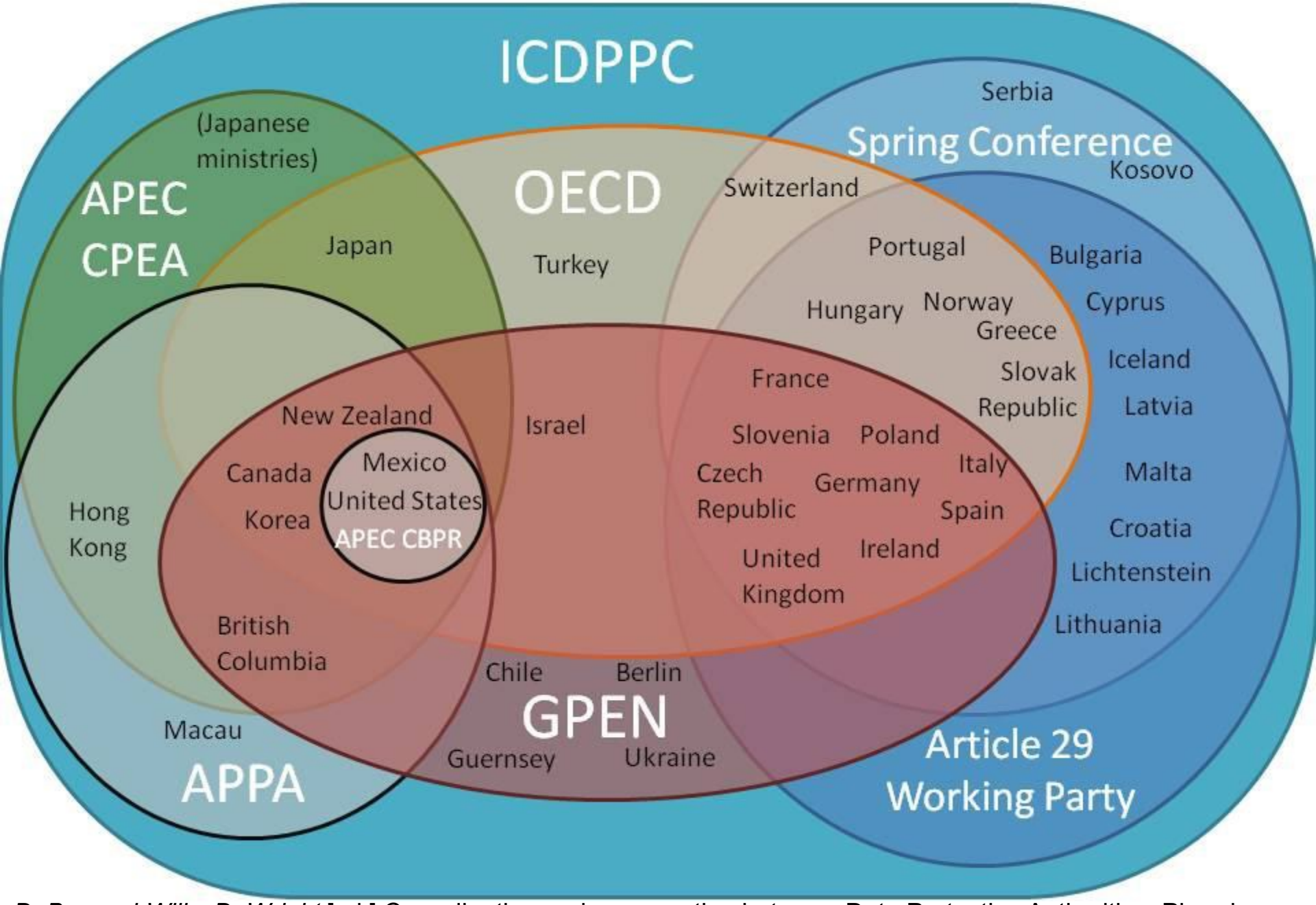
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Art. 5 GDPR

European co-operation of data protection authorities (DPAs)



EDPS



D. Barnard-Wills, D. Wright [ed.] Co-ordination and co-operation between Data Protection Authorities. Phaedra Workstream 1 report, 2014, p. 136

The Article 29 Working Party on the road to EDPB

- 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 on the road to EDPB

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

EDPS

The Article 29 Working Party on the road to 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.

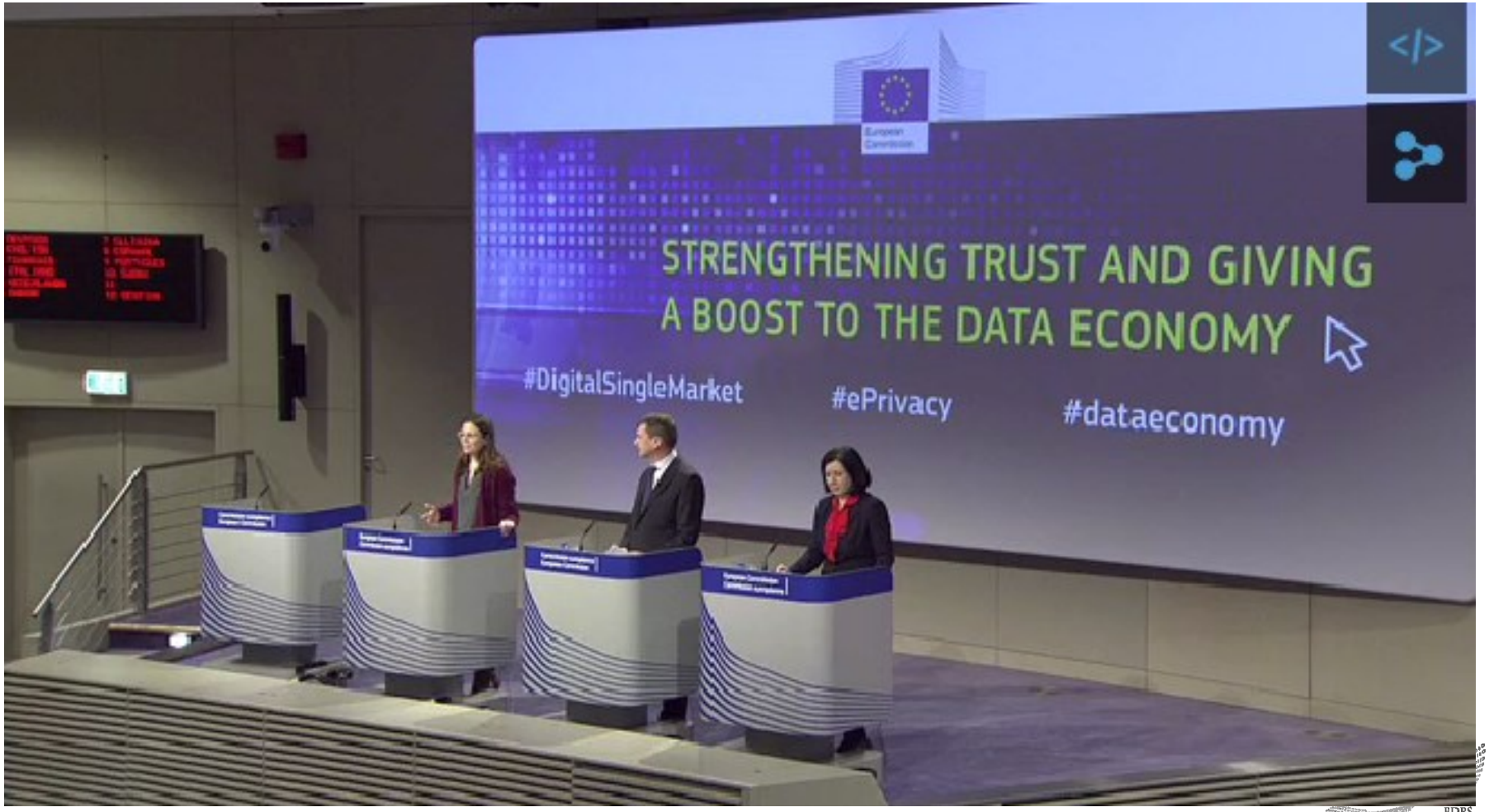
The Working Party will continue to analyze and provide its opinion on relevant subject matters under the current Directive 95/46/EC which either have already been on the previous work programme and should be maintained or are new topics to be dealt with in the two upcoming years.

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.

What else should happen now ?
Data protection in EU institutions

"New Regulation 45/2001"

What else should happen now ?
ePrivacy Regulation



What else should happen now ?
European Electronic Communication Code (???)

Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) - COM(2016)590 - September 2016

What else should happen now ?
”Cybersecurity Act”

COM(2017) 477 final 2017/0225(COD)

Proposal for a
Regulation of the European Parliament and of the Council
on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

What else should happen now ?
GDPR to be ”implemented” in Member States

What else should happen now ?
EFTA decission

The territorial application of the Data Protection Directive extends beyond the 28 EU Member States, including also the non-EU Member States that are part of the European Economic Area (EEA) – namely Iceland, Liechtenstein and Norway.

What else should happen now ?
Review of adequacy decisions

Andorra - 2010/625/EU

Argentina - 2003/490/EC

Canada - 2002/2/EC

Switzerland - 2000/518/EC

Faroe Islands - 2010/146/EU

Guernsey - 2003/821/EC

Israel - 2011/61/EU

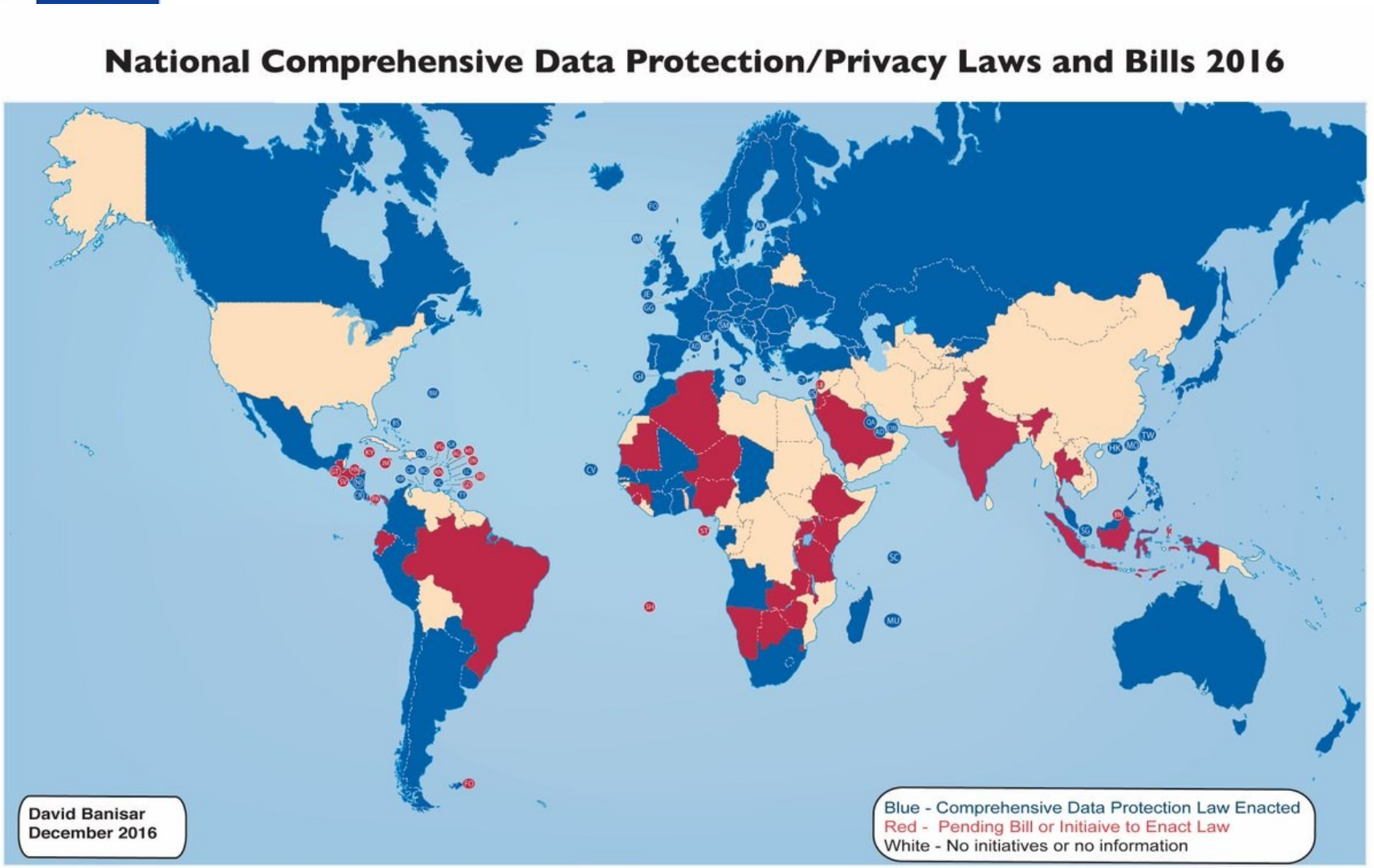
Isle Man - 2004/411/EC

Jersey - 2008/393/EC

New Zaeland - 2013/65/EU

United States – "Privacy Shield"

Data protection laws all over the world

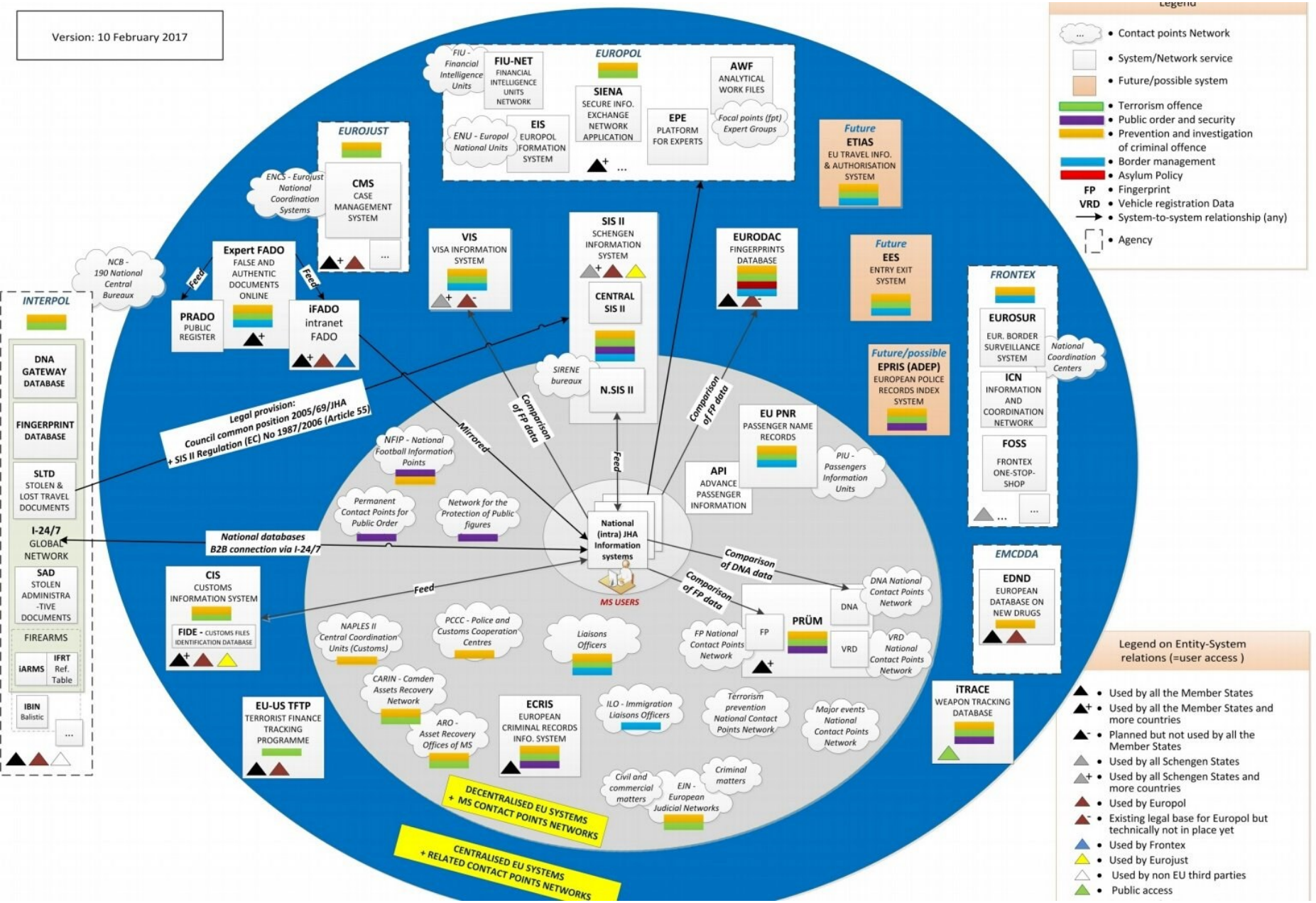


D. Banisar, *National Comprehensive Data Protection/Privacy Laws and Bills 2016* (as it stands for 28,11.2016).
See SSRN: https://ssrn.com/abstract=1951416 lub http://dx.doi.org/10.2139/ssrn.1951416

What else should happen now ?
Rules of procedure for EDPB

What is going on at the same time

1. *Data flow communication from the Commission*
2. *Japon starts its adequacy procedure*
3. *Korea invited to the discussion on adequacy*
4. *Review of Privacy Shield*
5. *Reform of Schengen Information System*
6. *Interoperability of the large scale IT systems in the EU*
7. *European Travel Information and Authorisation System (ETIAS)*
8. *e-Justice Directive (???)*



Overview of the information exchange environment in the justice and home affairs area, Nota Sekretariatu Generalnego Rady UE do delegacji z 15.2.2017 r. 6253/17, s.3, https://db.eurocrim.org/db/en/doc/2698.pdf

Codes of Conduct

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, **could be provided in particular by means of approved codes of conduct,** approved certifications, guidelines provided by the Board or indications provided by a data protection officer.

The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

Codes of Conduct

(98) **Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct**, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

Codes of Conduct

Section 5 **Codes of conduct and certification**

Article 40 **Codes of conduct**

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended **to contribute to the proper application of this Regulation**, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.
2. **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 this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

Codes of Conduct

Article 40 **Codes of conduct**

h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

j) the transfer of personal data to third countries or international organisations; or

k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing,

[…]

7. **Where a draft code of conduct relates to processing activities in several Member States**, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

[…]

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union.

Thank you for your attention!

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS