The Data Privacy Challenge: How Revenue Agencies are Coping in an Age of Risk and Innovation

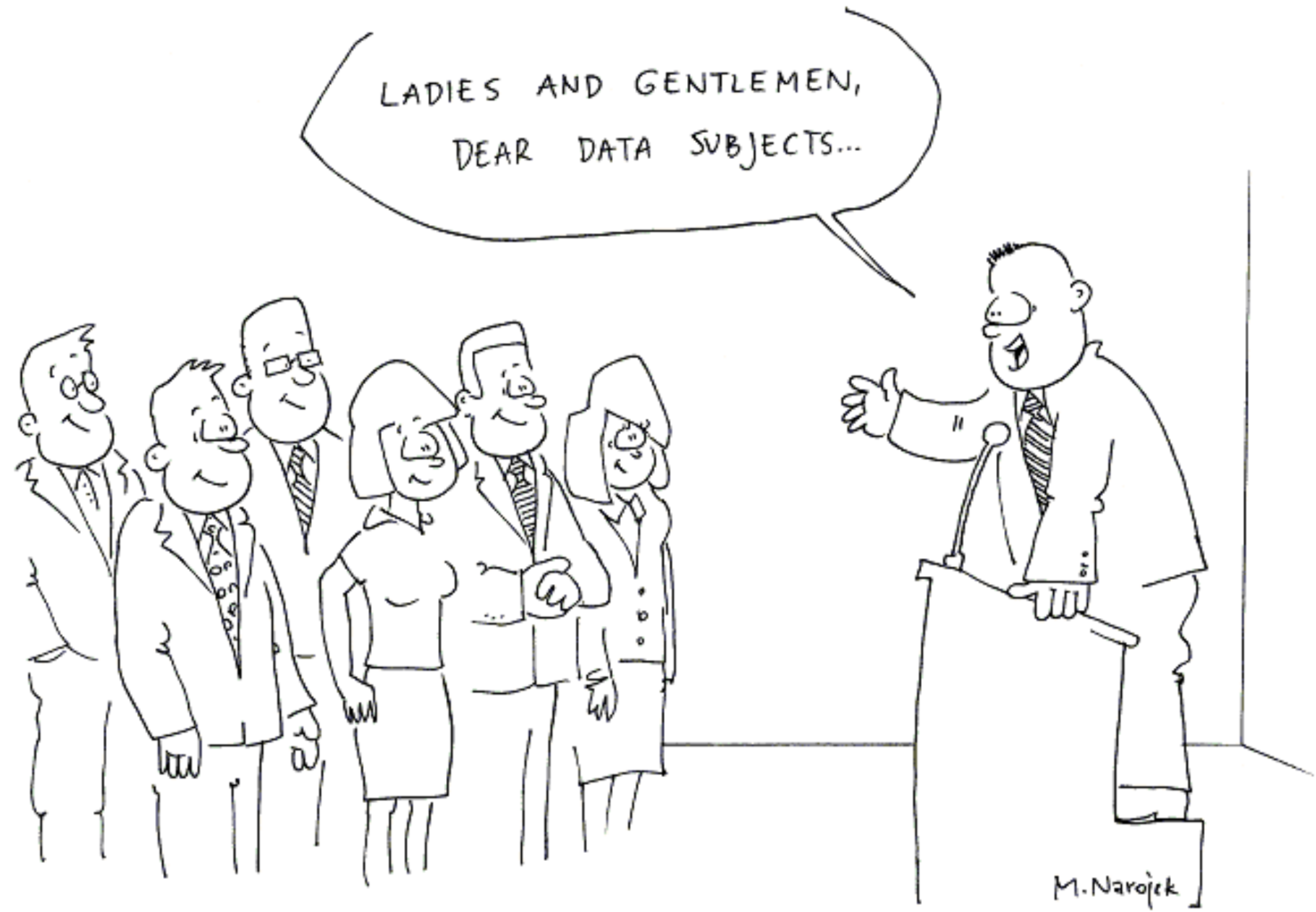
16/4/2018, Brussels

Wojciech R. Wiewiórowski

European Data Protection Assistant Supervisor

Tax and Revenue Collection in the Era of Data Protection: How Agencies Can Make Challenge an Opportunity.

High-Level Roundtable for Government Executives



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

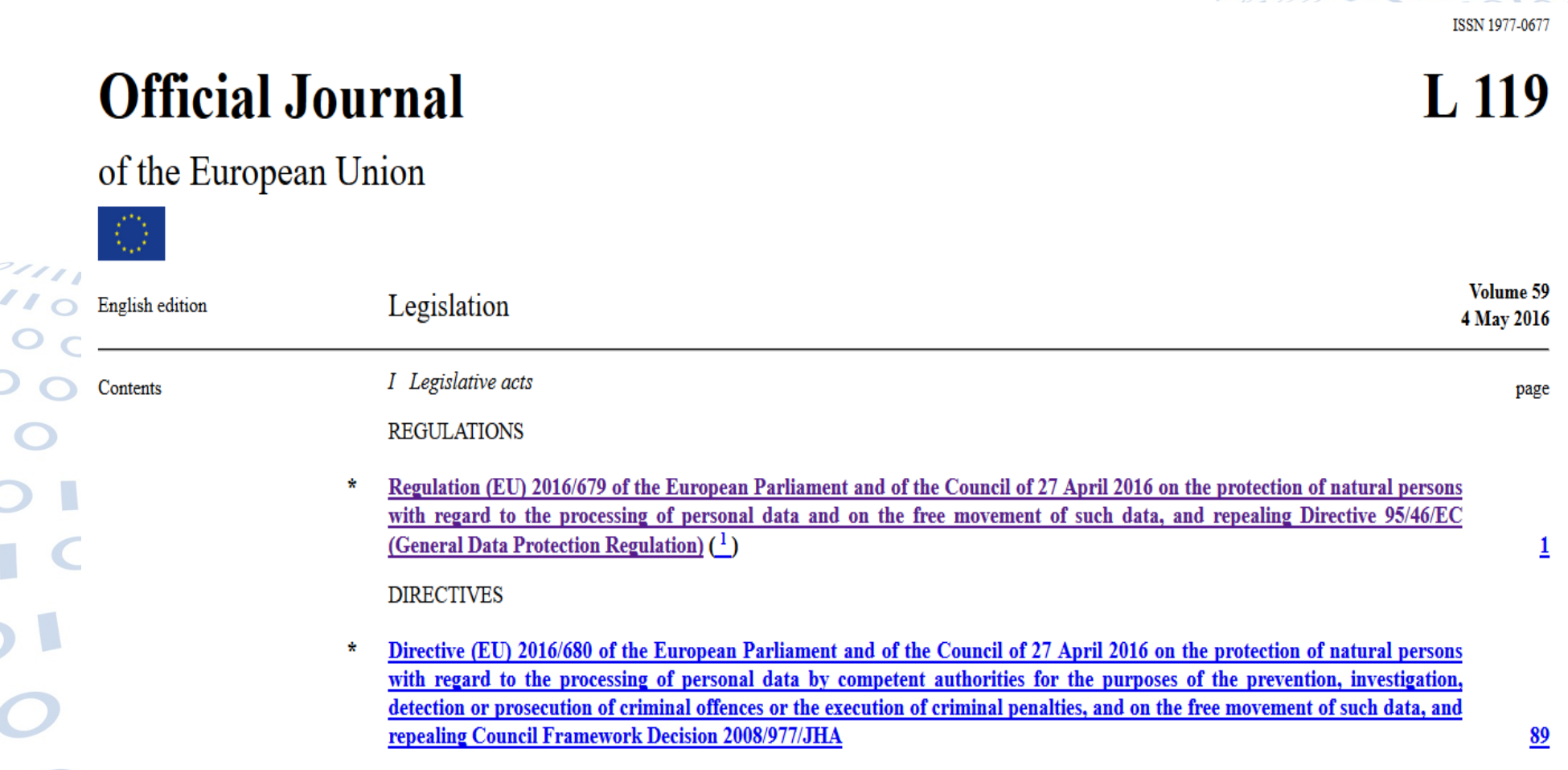
III. Opening a new chapter for EU data protection

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.

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 — page

I Legislative acts

REGULATIONS

* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ([1]) — 1

DIRECTIVES

* Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA — 89

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

Big data: Nihil novi sub sole?

‘Poured into huge computers, swapped with mountains of other data from other sources, tapped at the touch of an electronic code button, these vast reservoirs of personal information make it possible for government to collect taxes, for banks and schools and hospitals to serve millions of customers and students and patients, for restaurants and airlines and stores to extend immediate credit to people they've never seen before. But somewhere in the roil of expanding population, vast economy, foliating technology and chronic world crisis, individual Americans have begun to surrender both the sense and the reality of their own right to privacy— and their reaction to their loss has been slow and piecemeal. "The individual is being informationally raped," says a Michigan law professor whose career has been given over to the defense of privacy. "The government, credit bureaus, the police and others have their fangs in this guy. They each have their piece of information about this guy, and he doesn't have access to the information”’

The quote comes from Newsweek, the cover article entitled 'Is Privacy Dead?' in 1970.

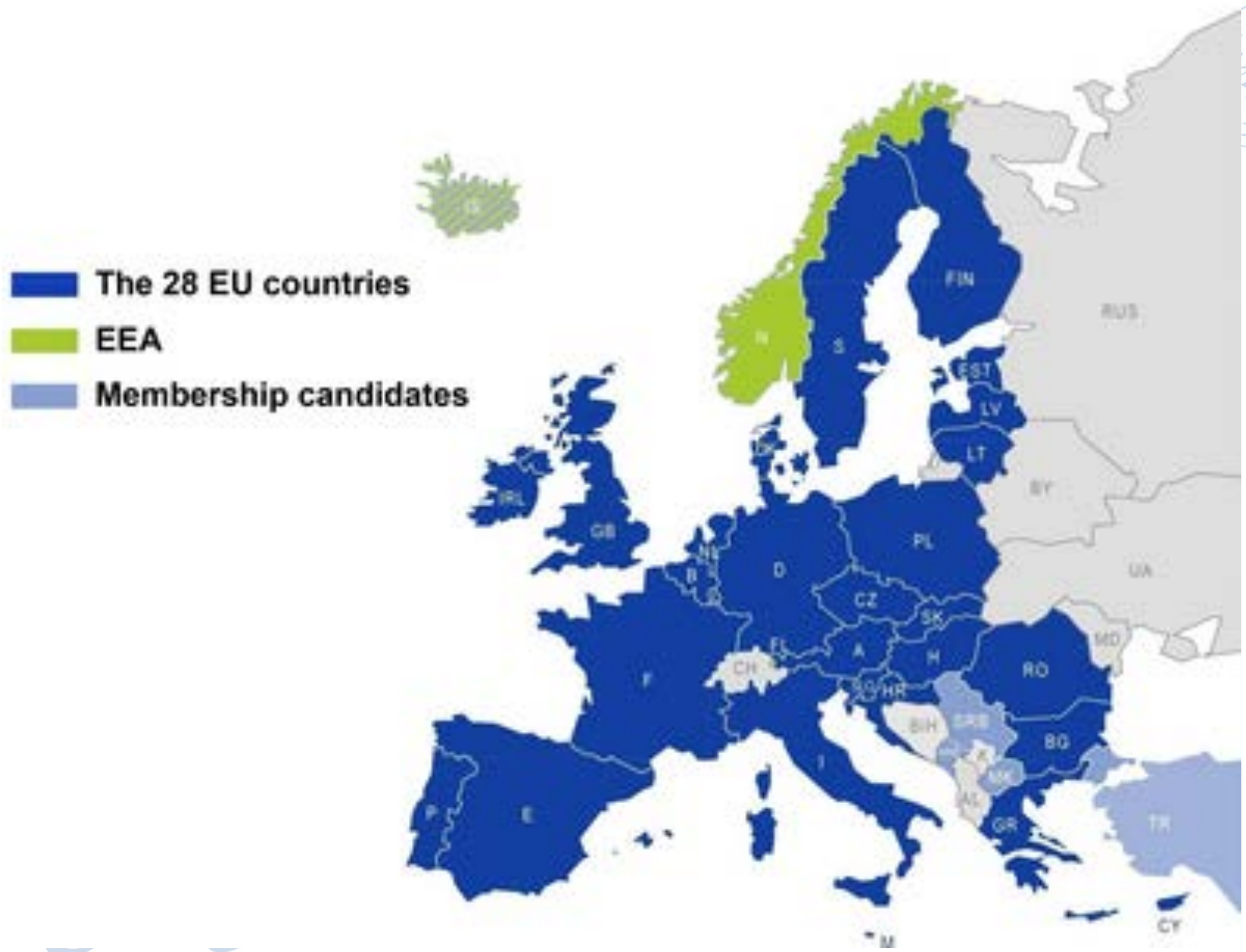
Big Data = Big Responsibility

Personal data - GDPR

(2) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person;

Convention 108 – Council of Europe

European co-operation of data protection authorities (DPAs)



EDPS

GDPR and public services - profiling

Building profiles according to Group of Art. 29

There are two main approaches to building user profiles:

i) ***Predictive profiles are***

established by inference from observing individual and collective user behaviour over time, particularly by monitoring visited pages and ads viewed or clicked on.

ii) ***Explicit profiles***

are created from personal data that data subjects themselves provide to a web service, such as by registering.

Both approaches can be combined. Additionally, predictive profiles may be made explicit at a later time, when a data subject creates login credentials for a website.

Opinion of Art. 29 WP, 2/2010 on behavioural advertising adopted on June 22 , 2010, page 8

GDPR and public services - profiling

Profiling is generally used in order to

1. get a sociologic and psychologic assessment of the client
2. discover material and social status of the client
3. create suggestions and strategies to be used in marketing activities

I would accept such explanation of profiling for marketing purposes

…. but …..

….. This is a thesis of FBI experts on criminal profiling.
I have just exchanged notions ”ofender” v. ”client” and ”investigation” v. ”marketing activites” ☺

R. M. Holmes, S.T. Holmes: Profiling Violent Crimes: An Investigative Tool , 4th Ed.,Thousand Oaks: Sage Publications, Inc. 2008

GDPR and public services - profiling

GDPR and public services - profiling

GDPR and public services - profiling

"Profile" refers to a set of data characterising a category of individuals that is intended to be applied to an individual.

(**GDPR**) 'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;.

GDPR and public services - profiling

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. **Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.**

GDPR and public services - profiling

(71) (…) However, decision-making based on such processing, including profiling, should be allowed **where expressly authorised by Union or Member State law** to which the controller is subject, **including for fraud and tax-evasion monitoring** and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

GDPR and public services - profiling

(71) (…) In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

GDPR and public services - profiling

Article 22 - Automated individual decision-making, including profiling

1. The data subject shall have **the right not to be subject to a decision based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is **authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard** the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the **data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests,** at least the **right to obtain human intervention on the part of the controller,** to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

GDPR and public services - profiling

Article 9 **Processing of special categories of personal data**

1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2.Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

GDPR and public services - profiling

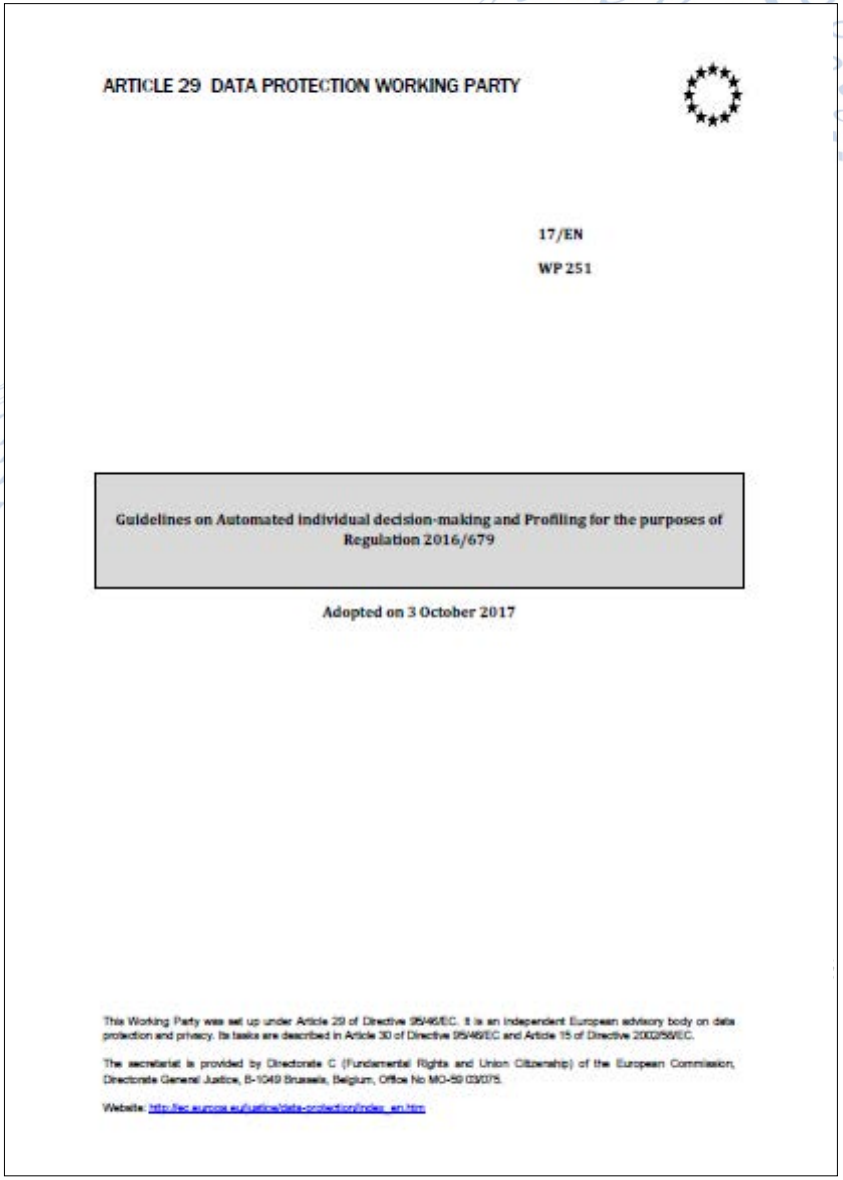
The Article 29 Working Party has adopted new guidelines covering profiling and automated decision-making under the forthcoming GDPR.

The guidelines acknowledge general benefits of these technologies:

a) increased efficiencies and

b) resource savings.

However, the WP29 warns that profiling and automated decision-making technologies can pose “significant risks for individuals’ rights and freedoms” and can “perpetuate existing stereotypes and social segregation” absent appropriate safeguards.



ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 251

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

Adopted on 3 October 2017

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 03/075.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Purpose imitation in public sphere

- The purpose for processing of personal data must be known and the individuals whose data is processed by a public administration must be informed. It is not sufficient to simply indicate that personal data will be collected and processed.

- When processing personal data a public administration must respect the purpose limitation principle, which requires that personal data must be collected for specified, explicit and legitimate purposes.

- It cannot be further processed in a manner which is incompatible with those purposes.

Purpose imitation in public sphere

- A novelty in the GDPR is that Article 6(4) also codifies an exception to the principle of purpose limitation for the case if the further processing is based on consent or Union or Member State law.

- However, this is not an open-ended permission to enact any sweeping and generic legislative text to allow for unlimited reuse of personal data across government departments. In line with the Charter of Fundamental Rights, the law must meet certain requirements if the principle of purpose limitation is to be derogated from. In particular, it must "*constitute a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)".*

- Moreover, under the GDPR, consent can only be relied upon as a processing ground, where consent is specific, informed, unambiguous and freely given.

- It will not usually be appropriate for public administration to rely upon consent as a processing ground. This is because there is likely to be a clear imbalance of power between the public authority and the individual.

The 'once-only' principle

the possibility to share personal data across public services for different purposes

- The ‘once-only’ principle aims to ensure that citizens and businesses are requested to supply the same information only once to a public administration, which can then re-use the information they already have.

- The EDPS’ opinion on the Proposal for the Regulation establishing a digital single gateway and the 'once-only' principle and considers the Proposal as an important initiative that aims to facilitate citizens' and businesses' cross-border activities through the modernisation of the public administrative services.

- The opinion provides recommendations on a range of issues, focusing on the legal basis of the processing for the cross-border exchange of evidence, purpose limitation, data subject rights and the scope of the ‘once-only principle’ as well as practical concerns surrounding user control.

- EDPS supports the efforts made to ensure that individuals remain in control of their personal data, including by requiring ‘an explicit request of the user’ before any transfer of evidence between competent authorities and by offering the possibility for the user to ‘preview’ the evidence to be exchanged.

Data subjects and right to information
(the CJEU in the judgment in Case C-201/14 Smaranda Bara and Others)

- CJEU judgment in Case C- 201/14 Smaranda Bara and Others provided the Court with the opportunity to elaborate on the right to information of individuals (data subjects) prior to and following the transfer of their personal data between public authorities.

- The Court observes that the National Health Insurance Fund's processing of data transferred by the tax authority required informing the data subjects of the purposes of that processing and the categories of data concerned. In this case, the Health Insurance Fund had not provided that information.

- The Court holds that EU law precludes the transfer and processing of personal data between two public administrative bodies without the persons concerned (data subjects) having been informed in advance.

- Prior to processing personal data, individuals must be informed by a public administration about the processing, such as its purposes, the types of data collected, the recipients, and their data protection rights.

Thank you for your attention!

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS