"Views of the EDPS on speech and data protection“

Sophia Antipolis, 29 January 2020

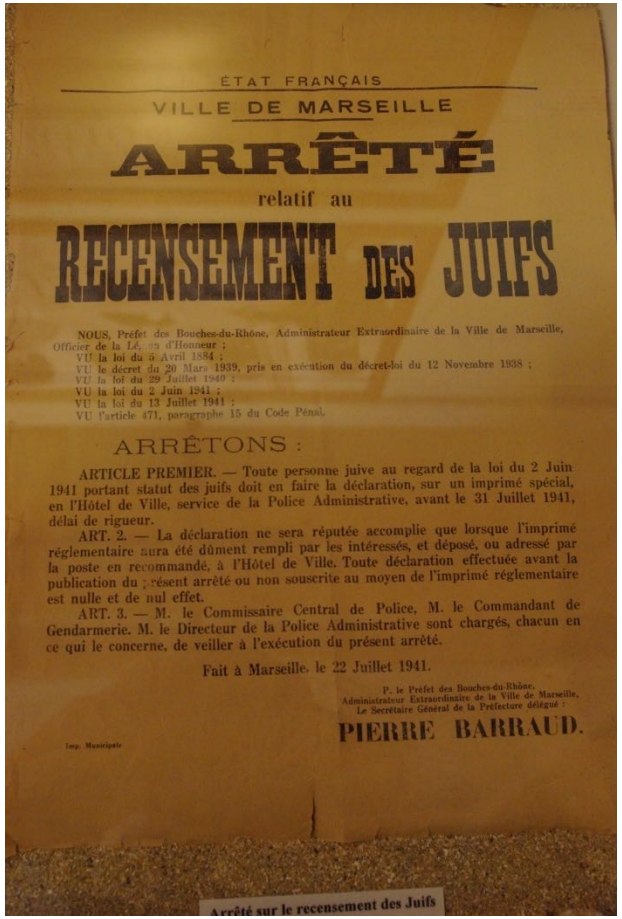
Thomas ZERDICK, LL.M.

Head of Unit “IT Policy”

European Data Protection Supervisor
thomas.zerdick@edps.europa.eu

Overview

1. The concept of “privacy“ in Europe
2. Private life and personal data protection
3. Speech and the GDPR



ÉTAT FRANÇAIS

VILLE DE MARSEILLE

ARRÊTÉ

relatif au

RECENSEMENT DES JUIFS

NOUS, Préfet des Bouches-du-Rhône, Administrateur Extraordinaire de la Ville de Marseille, Officier de la Légion d'Honneur ;
VU la loi du 5 Avril 1884 ;
VU le décret du 20 Mars 1939, pris en exécution du décret-loi du 12 Novembre 1938 ;
VU la loi du 29 Juillet 1940 ;
VU la loi du 2 Juin 1941 ;
VU la loi du 13 Juillet 1941 ;
VU l'article 471, paragraphe 15 du Code Pénal.

ARRÊTONS :

ARTICLE PREMIER. — Toute personne juive au regard de la loi du 2 Juin 1941 portant statut des juifs doit en faire la déclaration, sur un imprimé spécial, en l'Hôtel de Ville, service de la Police Administrative, avant le 31 Juillet 1941, délai de rigueur.

ART. 2. — La déclaration ne sera réputée accomplie que lorsque l'imprimé réglementaire aura été dûment rempli par les intéressés, et déposé, ou adressé par la poste en recommandé, à l'Hôtel de Ville. Toute déclaration effectuée avant la publication du présent arrêté ou non souscrite au moyen de l'imprimé réglementaire est nulle et de nul effet.

ART. 3. — M. le Commissaire Central de Police, M. le Commandant de Gendarmerie, M. le Directeur de la Police Administrative sont chargés, chacun en ce qui le concerne, de veiller à l'exécution du présent arrêté.

Fait à Marseille, le 22 Juillet 1941.

P. le Préfet des Bouches-du-Rhône,
Administrateur Extraordinaire de la Ville de Marseille,
Le Secrétaire Général de la Préfecture délégué :

PIERRE BARRAUD.

Imp. Municipale

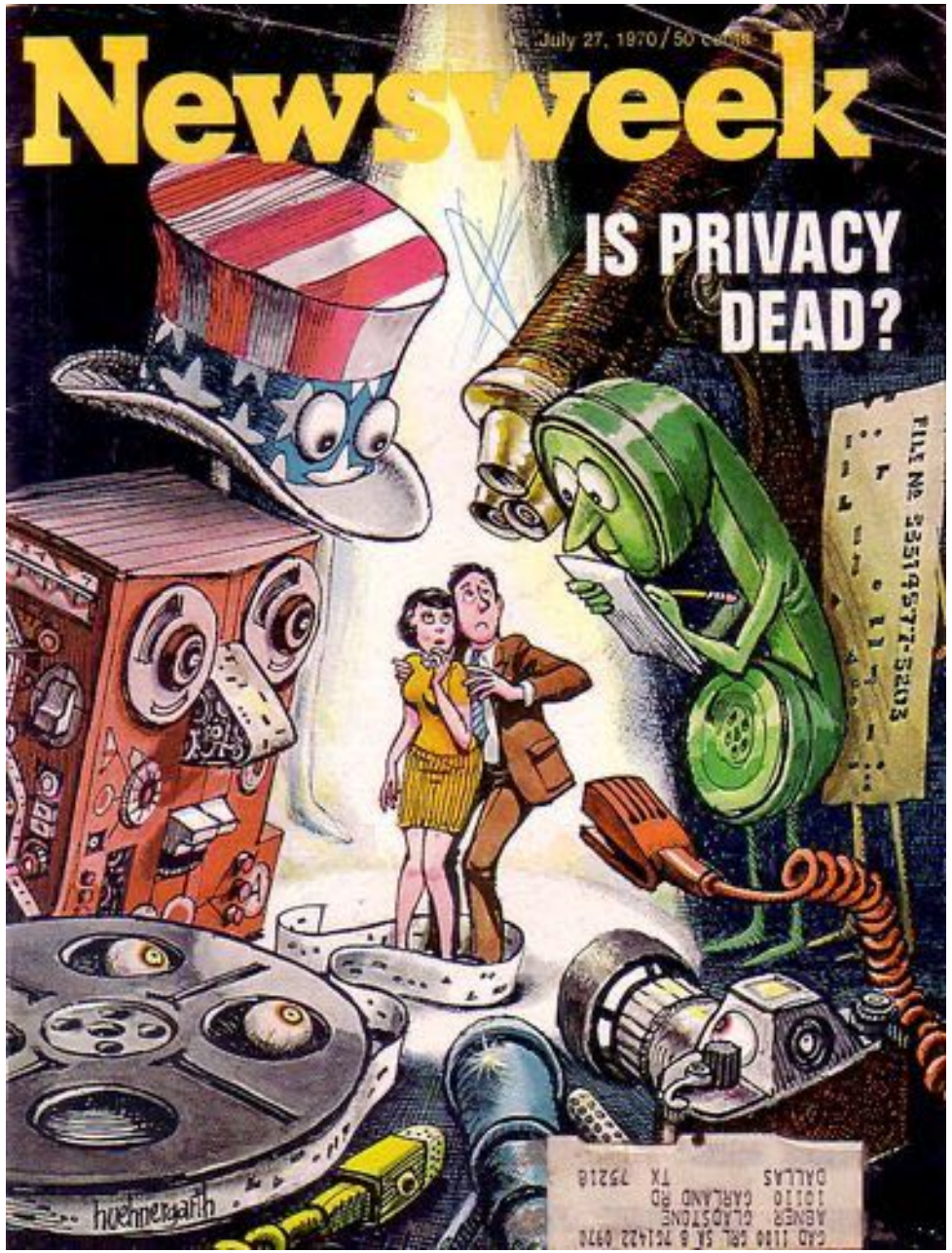
Arrêté sur le recensement des Juifs

- see also
- *Loi du 2 juin 1941 prescrivant le recensement des juifs publiée au Journal officiel du 14 juin 1941.*
- http://pages.livresdeguerre.net/pages/sujet.php?id=docddp&su=103&np=322

Ministry for State Security (*Ministerium für Staatssicherheit, MfS*)

https://www.stasimuseum.de/en/enindex.htm

‘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”’


Newsweek
July 27, 1970 / 50 cents
IS PRIVACY DEAD?
FILE № 235194577-5203
huemmergarth

European Convention of Human Rights

Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005

EU Charter of Fundamental Rights

- Article 7 - Respect for private and family life

- Everyone has the right to respect for his or her private and family life, home and communications.

http://data.europa.eu/eli/treaty/char_2016/oj

What is protection of personal data?

- An issue which involves everybody, individuals, states, companies
- A fundamental right issue
- A competitiveness issue

Beginnings of data protection

- 1960s: USA, two major reasons:
  - 1.) Technical progress based on the development of computers
  - 2.) Socio-political reason, raising fear of governmental surveillance “Big brother”
- Similar development in Europe
- 1970 – 1981
  - 1970: First law on data protection was enacted by the German Federal State of Hessen (07.10.1970).
  - Sweden (1973), Germany (1976), France (1978), Denmark (1978), Norway (1978), Austria (1978) and Luxembourg (1979) introduced national legislation on data protection
  - No role model as basis but had to be innovative in their own right

Beginnings of data protection (continuation)

- 1981 Council of Europe:
- Convention for the Protection of Individuals with regard to automatic processing of personal data (entry into force 1985)
  - First internationally binding instrument on data protection, important point of orientation for the subsequent national data protection laws

- In the following years, data protection legislation was enacted by
  - Finland (1987), The Netherlands (1988), Portugal (1991), Spain (1992), Belgium (1992), Italy and Greece

International Data Protection (general)

- From 1948 privacy rights in various national and regional human rights bills
- From 1970 on data protection laws at national level
- 1980 OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  - Non-binding, orientation
- 1990 UN: Guidelines concerning computerized personal data.
  - Guidelines for orientation, procedure left to the initiative of each state

Directive 95/46/EC

- was the **reference text**, at European level, on the protection of personal data.
- sets up a **regulatory framework** which seeks to strike a balance between a **high level of protection for the privacy of individuals** and the **free movement of personal data** within the European Union (EU).
- provides a high level of protection of personal data and privacy, **regardless of the technologies used**.
- sets strict **limits on the collection and use of personal data**
- demands that each Member State set up an **independent national body** responsible for the protection of these data.
- (14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate **sound** and image data relating to natural persons, this Directive should be applicable to processing involving such data;

In the European Union, the protection of personal data is a fundamental right.

Article 8 EU Charter of Fundamental Rights

EU Charter of Fundamental Rights

Article 8 - Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

   Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Where is the **trust** ?

The two reform instruments

- The **General Data Protection Regulation** is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year.
- http://data.europa.eu/eli/reg/2016/679/2016-05-04

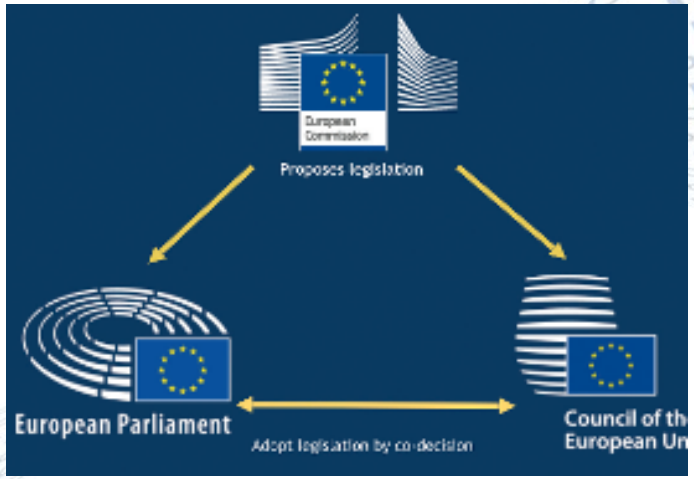
- The **Data Protection Directive for the police and criminal justice sector** protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. It will ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism.
- http://data.europa.eu/eli/dir/2016/680/2016-05-04

The new EU Legal Framework

For EU Member States

Since 25 May 2018:

- General Data Protection Regulation (GDPR)
- Police Directive,
- e-Privacy Directive, ...



For EU institutions, offices, bodies and agencies

Since 12 December 2018:

- Regulation (EU) 2018/1725

Regulation (EU) 2018/1725 [EDPR]	Regulation (EU) 2016/679 [GDPR]
Chapter I General Provisions	Chapter I General provisions
Chapter II General Principles	Chapter II Principles
Chapter III Rights of the Data Subject	Chapter III Rights of the Data Subject
Chapter IV Controller and Processor	Chapter IV Controller and Processor
Chapter V Transfers of personal data to third countries or international organisations	Chapter V Transfers of personal data to third countries or international organisations
Chapter VI European Data Protection Supervisor	Chapter VI Independent supervisory authorities
Chapter VII Cooperation and Consistency	Chapter VII Cooperation and Consistency
Chapter VIII Remedies, Liability And Penalties	Chapter VIII Remedies, Liability And Penalties
Chapter IX Processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU	Chapter IX Provisions relating to specific processing situations
Chapter X Implementing Acts	Chapter X Delegated acts and implementing acts
Chapter XI Review	Chapter XI Final provisions
Chapter XII Final provisions	

Key novel concepts of the GDPR

- 😉**Right to be forgotten and erasure**
- 😉**Right to data portability**
- 😉**Responsibility and Accountability**
- 😉**Data protection by design/ by default**
- 😉**Data breach notification**
- 😉**Data protection officer (DPO)**
- 😉**Data protection rules for police and law enforcement**

“Personal data“ means much more than “name and surname“

- 'personal data‘: **shall mean any information relating to an identified or identifiable natural person ('data subject');**
- an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- (Art. 4(1) GDPR)

“Processing“ means more than “collection”

- Definition:
  'processing of personal data‘('processing'):

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

  (Art. 4 No. 2 GDPR)

Biometric data

- ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

- (Art. 4 (14) GDPR)

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.

Data Protection Supervisory Authority

- Responsible for enforcing data protection legislation
- Set-up/ organisation to be decided by Member States, but must be in line with EU GDPR requirements
- Criteria + powers

- ‘Complete independence’ means:
  no government control or supervision.

The EDPS:
European Data Protection Supervisor

Ensures that EU institutions and bodies respect the fundamental right of data protection.

Wojciech Wiewiórowski
EDPS

Who are the actors?

Controller (one or more): responsible of the processing operation (determines purposes and means);

Processor (one or more): processes personal data on behalf of the controller(s);

Data subject: Natural person whose data are being processed.

Obligations of the controllers

Controller: responsible of the processing operation (determines purposes and means);

Document data processing operations, keep records and do risk assessments.

Be accountable for processing operations: demonstrate

Include security measures; inform data subjects about their rights

Principles of processing

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation (proportionality)
- Accuracy
- Storage limitation

New

- Integrity and confidentiality
- Accountability

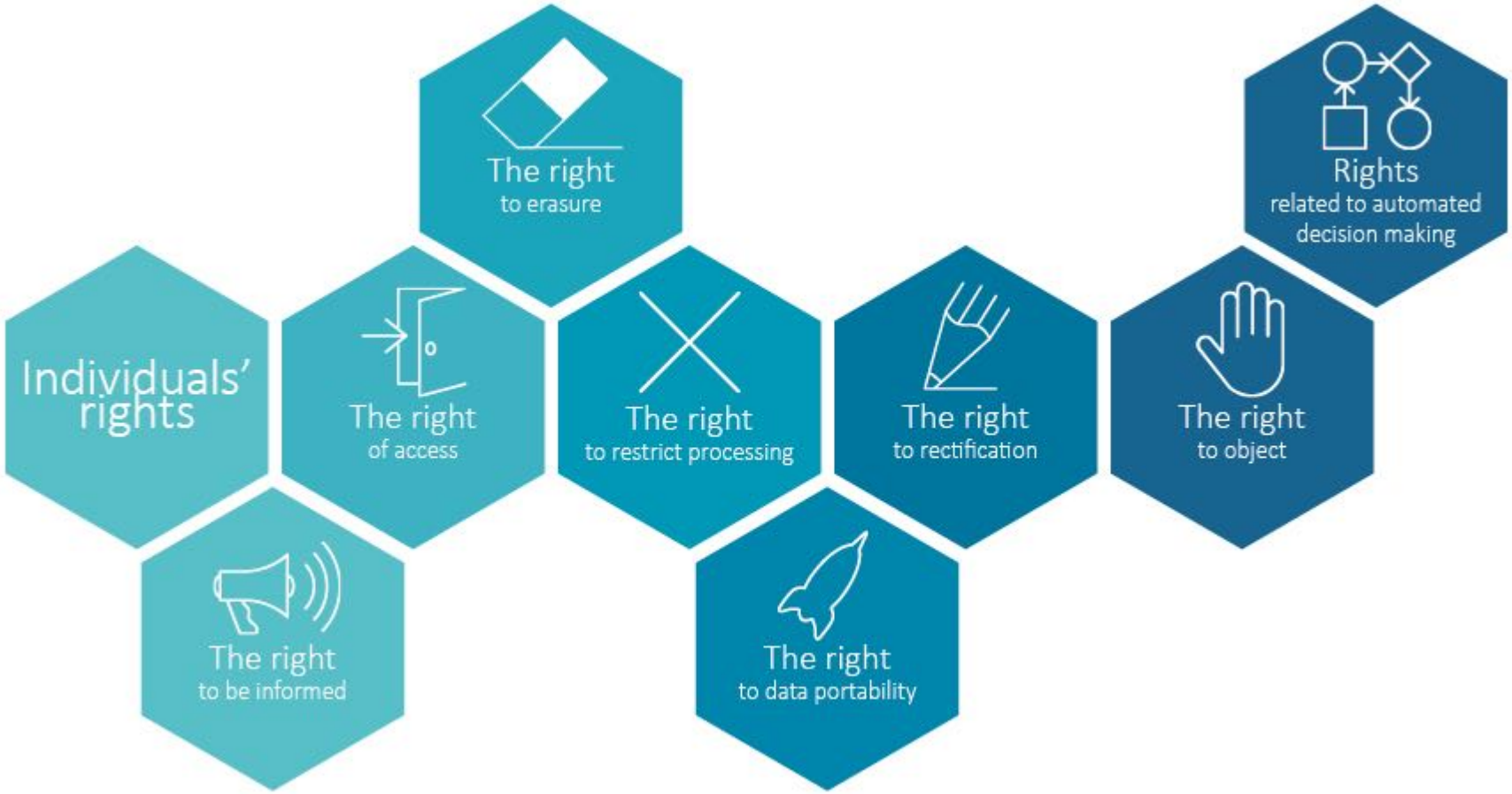
Principle of lawfulness

- Processing is necessary for:
  - the functioning of the EU institutions (compliance Treaty)/public interest;
  - compliance with a legal obligation;
  - the performance of a contract;
- Consent
- Protection of vital interest of the person
- legitimate interests of the controller (not in EDPR)

Putting you back in control

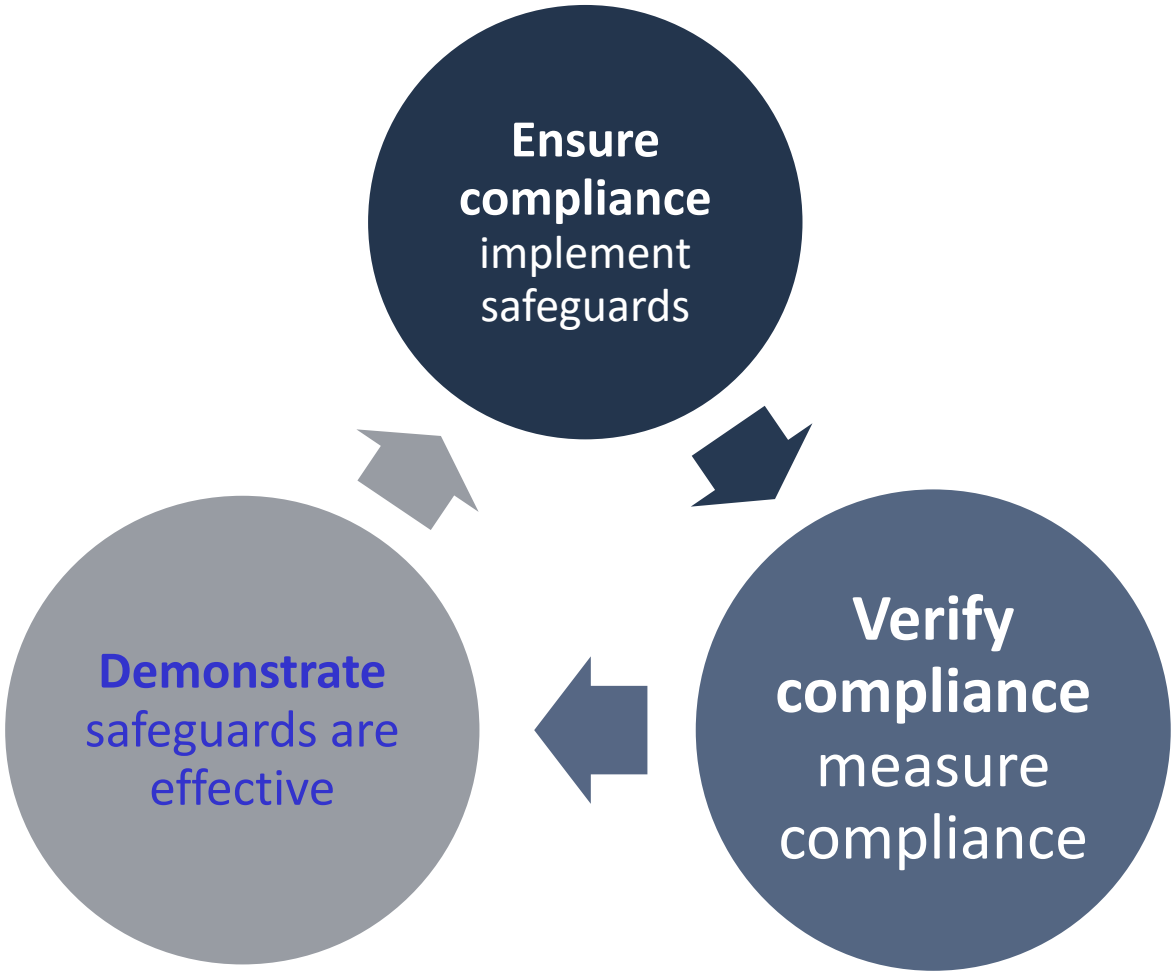
Under the new laws, you'll have more control over what happens to your data. And you'll know where to go and who to talk to if you're not happy.

Data protection - rights and principles



Accountability

Accountability



Embed data protection principles and safeguards

Data Protection by Design	"Implement data protection principles" "both at the time of the determination of the means for processing and at the time of the processing itself"
Data Protection by default	= strictest privacy settings automatically apply
➔ Common sense + **think data protection!**	E.g. Recruitment manuals, requests for supporting documents, databases, online forms...

From Privacy by design …
… to data protection by design

- PbD
  - Approach developed since 1995
  - High level framework
  - Difficult to enforce
- GDPR approach
  - Data protection by Design and by Default
  - DPbDD, DPbD
  - Based on accountability and DP principles
  - Legal obligation
  - Violation may be fined ≤ max(10 M€; 2% of turnover)
  - Certification of compliance

GDPR Article 25, paragraph 1:

"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing,

the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself,

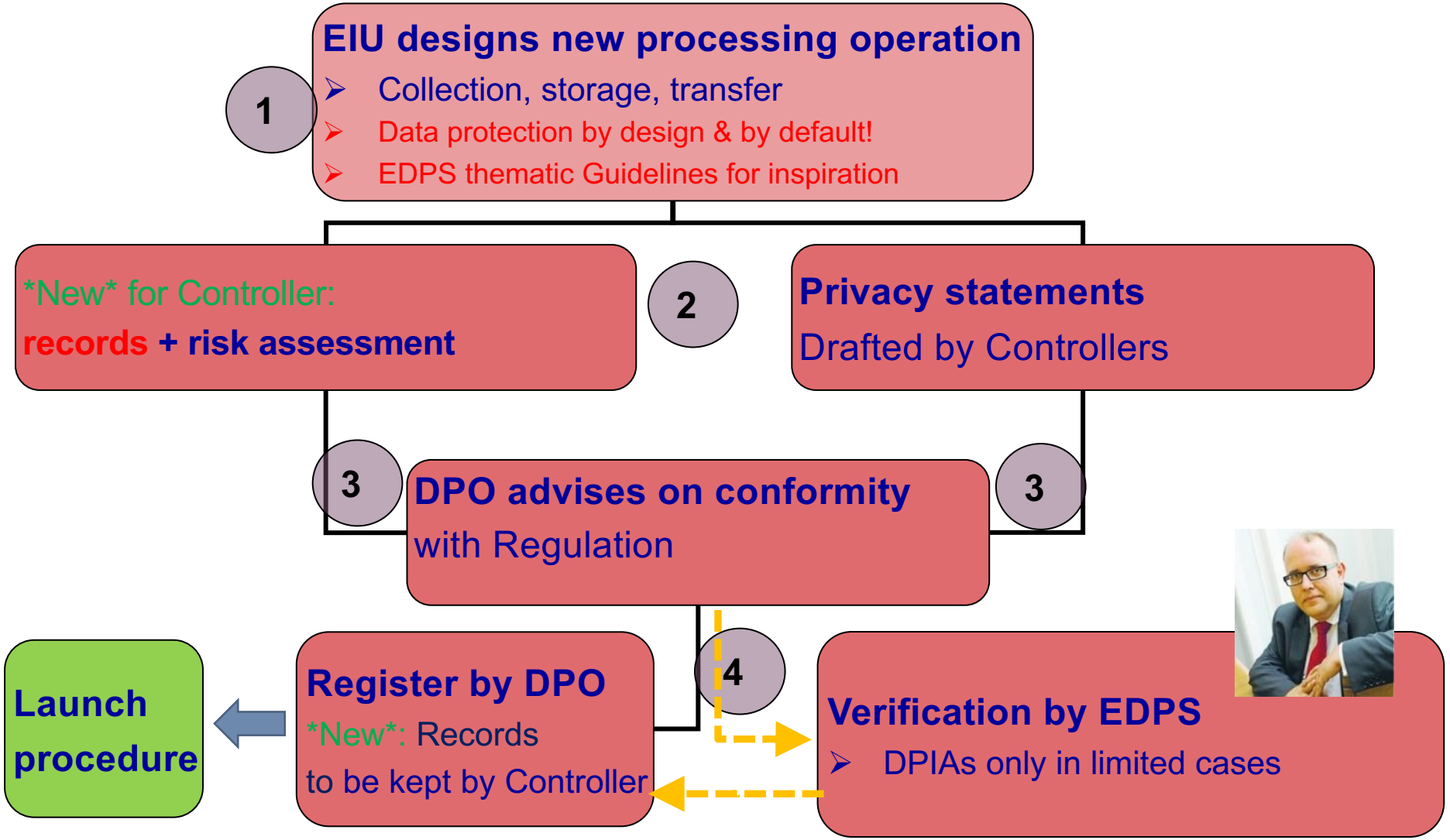
1. **implement appropriate technical and organisational measures**, such as pseudonymisation,
2. **which are designed**
3. **to implement data-protection principles**, such as data minimisation, **in an effective manner** and
4. **to integrate the necessary safeguards** into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

“Demonstrate”: records

“Demonstrate”:
Information through privacy statements

Data Protection Impact Assessment (DPIA)

In a nutshell



What happens if your data gets lost or stolen?

At the moment, if your data is lost or stolen, it may take some time for you to find out. In future if this happens, and the consequences are expected to be serious, then both you and your country's Data Protection Authority will have to be told as soon as possible.

Personal data breach notifications

YAHOO!

NOTICE OF DATA BREACH

Dear Yahoo user,

We are writing to inform you about a data security issue that may involve your Yahoo account information. We have taken steps to secure your account and are working closely with law enforcement.

What happened?

In November 2016, law enforcement provided Yahoo with data files which a third party claimed was Yahoo user data. We analysed this data with the assistance of external forensic

The Data Protection Officer

Two-fold role:

- Ensures that controllers and processors are informed of their obligations;
  (notification of data processing operations, implementing security measures..)

- Ensures that data subjects are informed of their rights;
  (right of access, rectification, blocking, erasure etc.)

信用中国
CREDITCHINA.GOV.CN

信用信息 统一社会信用代码 站内文章

请输入企业/法人名称或统一社会信用代码查询

农业农村部：不得截留套取和冒领农牧民补助奖励资金

专栏 头条新闻 中国新闻网 | 2019/05/10

据农业农村部网站消息，日前，农业农村部办公厅印发《关于进一步做好农牧民补助奖励政策落实工作的通知》(以下简称《通知》)。《通知》要求，严格执行资金专账管理、专项核算制度，确保资金专款专用，不得截留套取和虚报冒领。

查看详情 >>

Profiles

“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.

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.

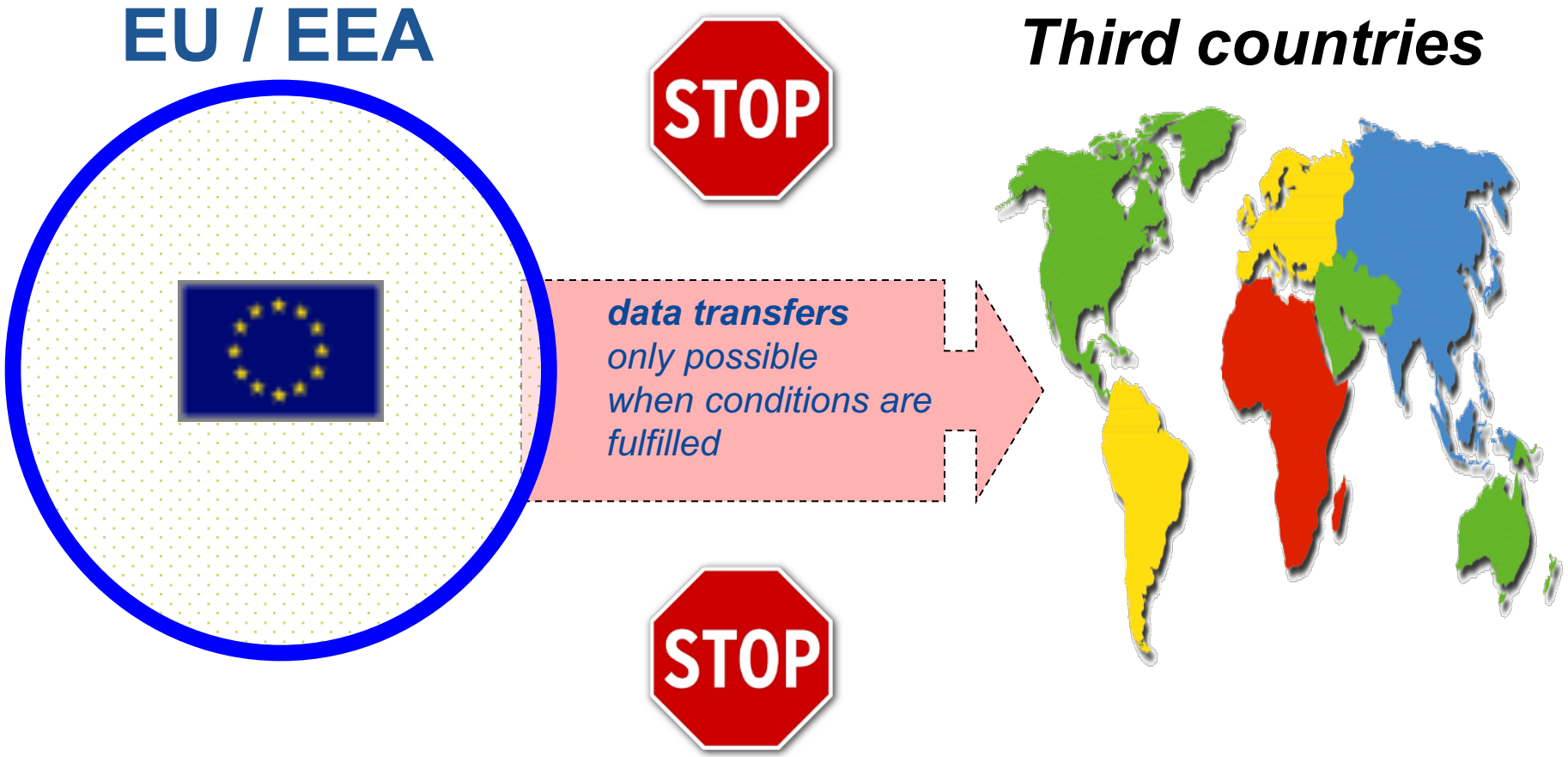
2. Paragraph 1 shall not apply if the decision:
   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
   (b) is **authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard** the data subject's rights and freedoms and legitimate interests; or
   (c) is based on the data subject's explicit consent.

Article 22 - Automated individual decision-making, including profiling

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.

Transfers of personal data



Protection of electronic communications

- The **ePrivacy Directive** builds on the EU telecoms and data protection frameworks to ensure that all communications over public networks maintain respect for fundamental rights, in particular a high level of data protection and of privacy, regardless of the technology used.
- https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML

- Proposal for a **ePrivacy-Regulation**
- https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications


I CAN'T KEEP
CALM
BECAUSE
I WANT
MORE

Resources on personal data protection

- **Handbook on European data protection law**

- Avalaible in
- BG DE EL EN ES FR HU IT

EDPS TechDispatch

To subscribe (*free*!):
https://edps.europa.eu/data-protection/our-work/our-work-by-type/techdispatch_en

TechDispatch #1: Smart Speakers and Virtual Assistants
TechDispatch #2: Smart Meters in Smart Homes
TechDispatch #3: Connected Cars

EDPS WEC

Website
Evidence
Collector

https://edps.europa.eu/press-publications/edps-inspection-software_en

"Introduction to the hash function as a personal data pseudonymisation technique"

(paper available in EN and ES)

https://edps.europa.eu/node/5553

Privacy by design

- EDPS Preliminary Opinion on Privacy by Design
- Available in EN, DE, FR
- https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en

EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Adopted on 13 November 2019

- Background, interpretation, examples
- 11 recommendations

https://edpb.europa.eu

EDPS IPEN workshops

- Focus on
- **“State of the art”**
- **Business without tracking**
- **Privacy engineering methodologies**
- **Anonymisation, pseudonymisation**

https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en

Thank you!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor