Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Enrique Gaspar San José

Transfers of personal data to third countries

Madrid, 15 February 2023

The project is co-financed with the support of the European Union's Justice programme

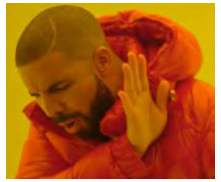
What is an International Transfer?

"Data transfer is an intentional sending of personal data to another party or making the data accessible by it, where neither sender nor recipient is a data subject"

Information Commissioner's Office (independent supervisory authority for data protection in the UK. Yeah, the UK used to be in the EEE)

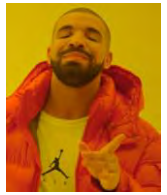
What parties can be involved in an International Transfer?

EXPORTER **IMPORTER**



I don't care whether you are a controller or a processor.

Is personal data of European subjects being transferred to or made available for countries outside the EEE without the data subject being one of the two parties?



That's what I care about.

GOVERTIS
Part of Telefónica Tech

Where are International Transfers regulated?

CHAPTER V

Unless you are a EUI

If so, go here

GOVERTIS
Part of Telefónica Tech

Where are International Transfers regulated?

GOVERTIS
Part of Telefónica Tech

How is it regulated in the GDPR?

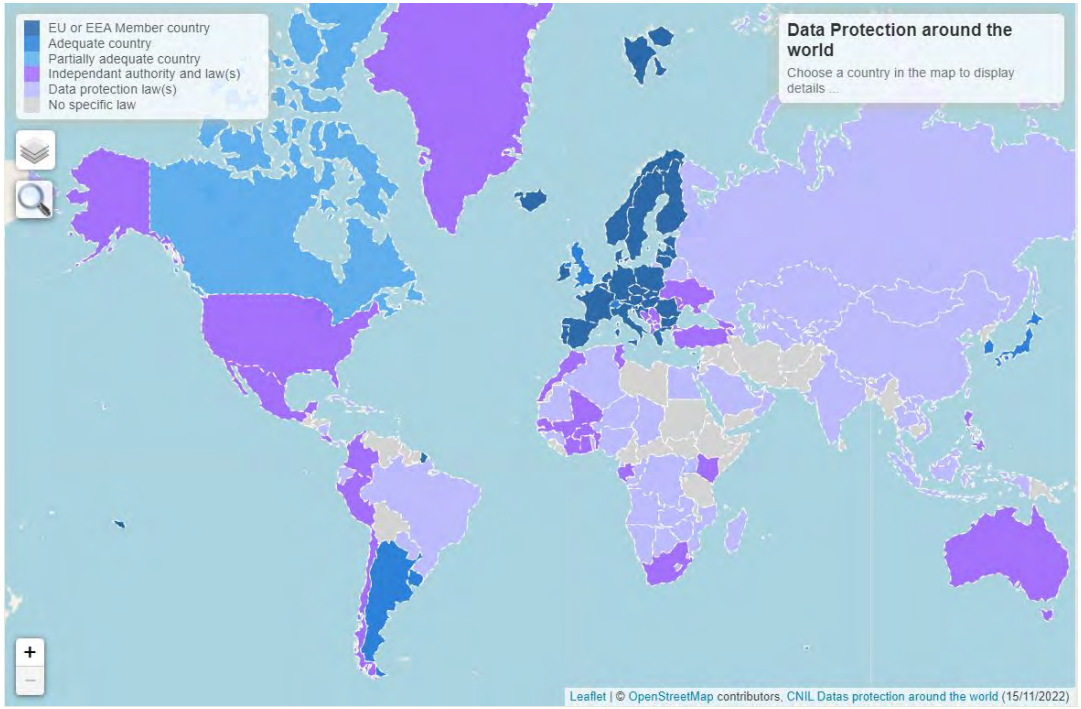
Art. 45: Adequacy decisions

Art. 46: Appropriate safeguards

Art. 49: Derogations

Art. 45: Adequacy decisions

1. A proposal from the European Commission
2. An opinion of the European Data Protection Board
3. An approval from representatives of EU countries
4. The adoption of the decision by the European Commission



[Data protection around the world | CNIL]

GOVERTIS
Part of Telefónica Tech

Art. 46: Appropriate safeguards

AKA Transfer tools

No DPA authorization

- Legally binding and enforceable instrument
- Binding corporate rules (art. 47 GDPR)
- Standard data protection clauses (SCCs)
- Approved code of conduct (art. 40 GDPR) + binding commitment to safeguards from importer
- Approved certification mechanism (art. 42 GDPR) + binding commitment to safeguards from importer

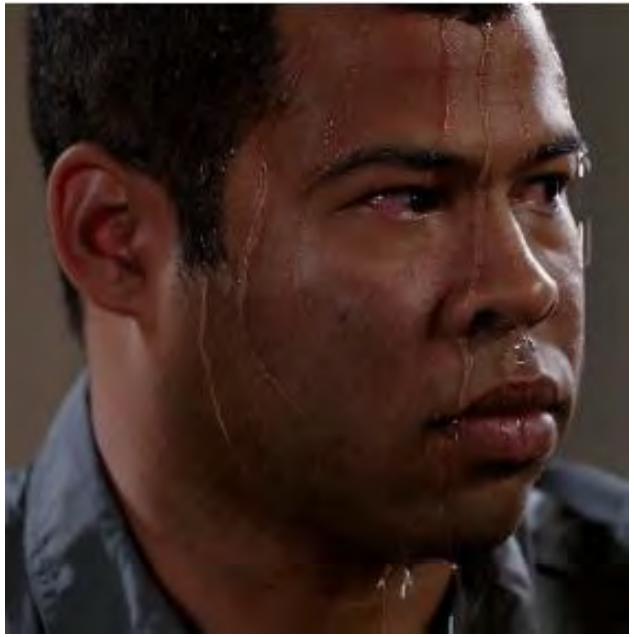
DPA authorization

- Ad-hoc Contractual Clauses
- Administrative Arrangements (not legally binding, like a memorandum)

Art. 49: Derogations

- Explicit consent to transfer
- Contract with data subject
- Contract in interest of data subject
- Important reasons of public interest
- Legal claims
- Vital interests of data subject/others
- Public register

Art. 49: Derogations



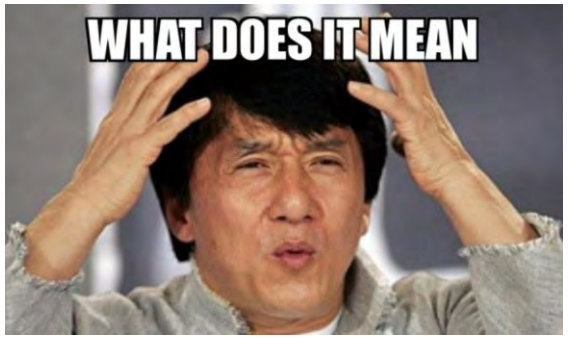
- Last resort
- Not repetitive
- Few data subjects
- Compelling legitimate interest of the controller > data subjects
- Assesment of required safeguards
- Controller has to inform both DPA and data subjects

Schrems II


BANNED
EU-US
privacy shield
WAIT, IT'S BEEN
INVALIDATED AGAIN?
ALWAYS
HAS BEEN

Schrems II

If you don't manage to guarantee an essentially equivalent protection, you can't do the transfer



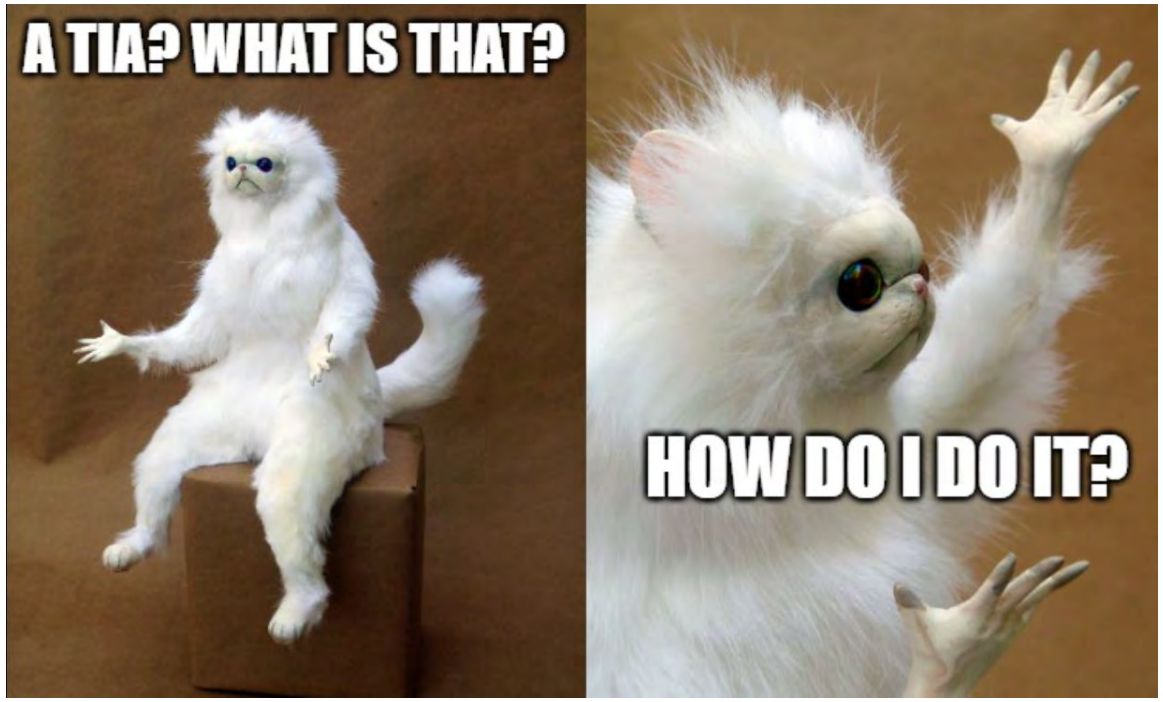
TRANSFER TOOLS

+

DATA TRANSFER IMPACT ASSESSMENT (TIA)

GOVERTIS
Part of Telefónica Tech

TIA

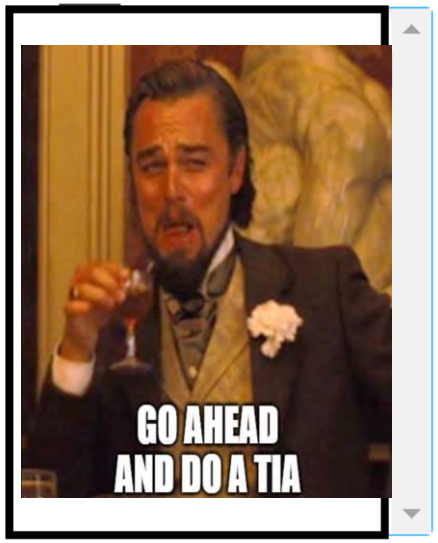


edpb
European Data Protection Board

RECOMMENDATIONS 01/2020

TIA

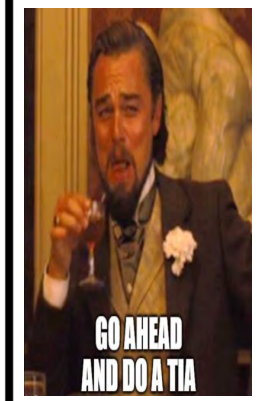
Product - Sub-Processors



- USA
- Canada
- UK
- **EU**
- Australia
- APAC
- USA/EU

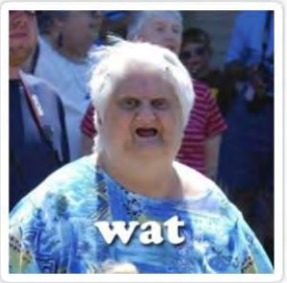
It's easy to say that you need to do a TIA

It's not so easy to do it

Product	Geogra...	Sub-Processors	Service-Location	Service	Vendor-Operations
	EU		EU (Frankfurt)	Data Center	
	EU		EU (Frankfurt)	Database Backups	
	EU		Massachusetts, US	CDN / WAF	
	EU		Chicago, US	APM	
	EU		EU	Logs	
	EU		AWS US	IDR	
	EU		US West (Oregon)	Email	
	EU		US West (Oregon)	Usage Data	
	EU		 US-East-1 (N. V...	Usage Data	
	EU		 US	Usage Data	

Google Analytics Case

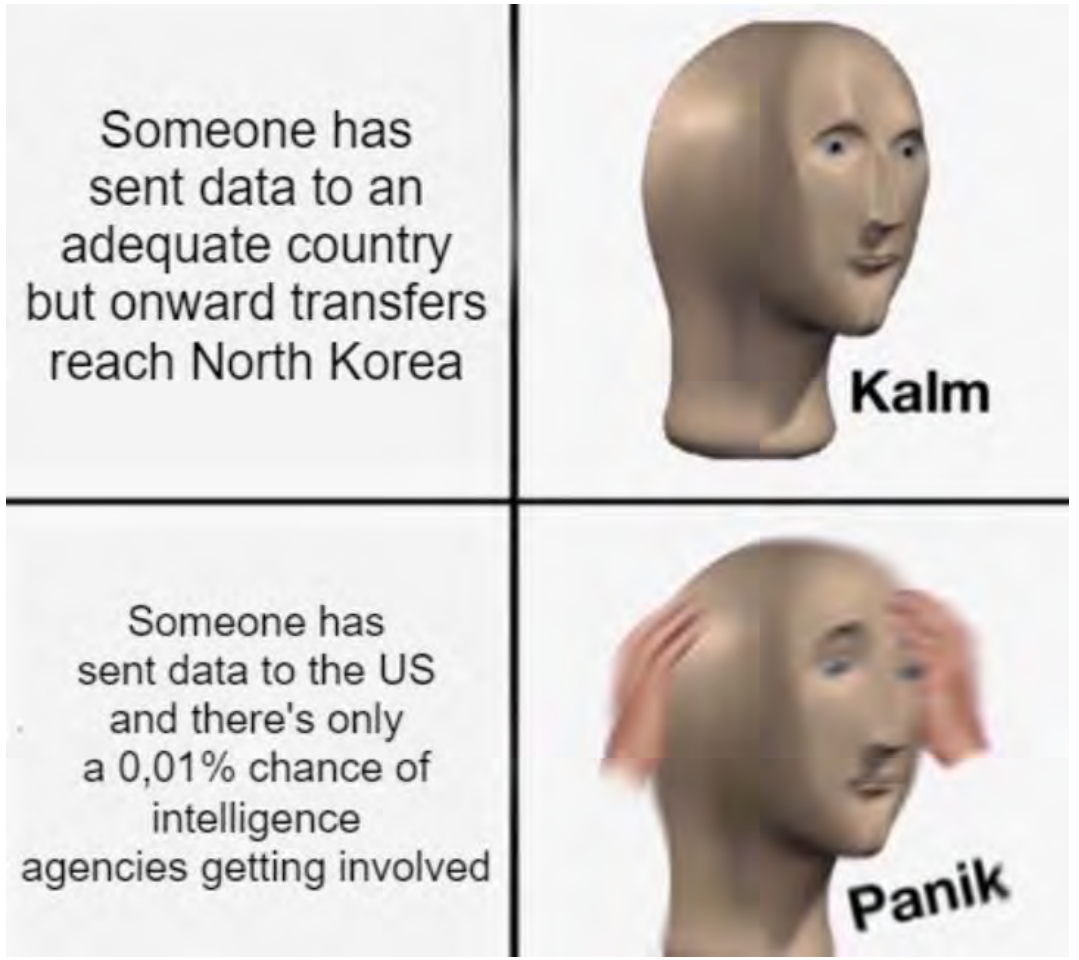
Chapter V of the GDPR doesn't accept... RBA?



Conclusions

Don’t worry

TIA is still the best tool we have in this very moment to do a safe transfer, when needed



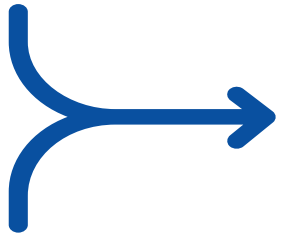
Conclusions

Q: Will we have a new Privacy Shield?
A: Sure
Q: Will it last?
A:

Conclusions

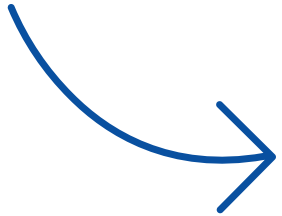
What could be the solutions?

- Consensus inside Europe
- Complete acceptance of RBA



We can't have different opinions between European Commission, EDPB and DPAs

- Main importers stablish infrastructure inside Europe.



It's not so far-fetched: EU Data Boundary for the Microsoft Cloud

THANK YOU VERY MUCH!

AND MAY YOUR TIAs BE ENOUGH

GOBERTIS
Part of Telefónica Tech

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Maitane Valdecantos

Data controller and processor

Madrid, 15 February 2023

The project is co-financed with the support of the European Union's Justice programme

Introduction

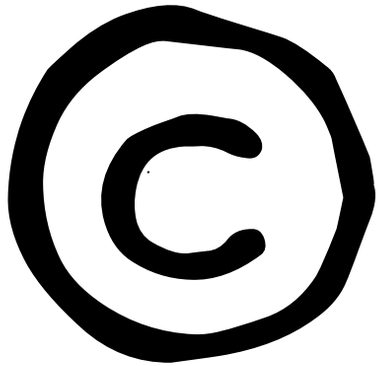
The concepts of controller, joint controller and processor play a crucial role in the application of the GDPR.

They determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice.

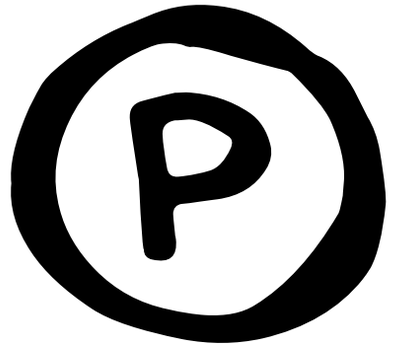
Guess who?

“Data controller” and “data processor”

The two main parties responsible for complying with the data protection laws are:



Data controller



Data processor

The data controller

Definition of data controller

"*The natural or legal person, public authority, agency or other body which, alone or jointly with others,* ***determines*** *the purposes and means of the processing of personal data*"

Art. 4.7) GDPR

Decision-making power

The key factor: the capacity to take decisions

It is not always easy to identify the ©.

The circumstances must be analysed to answer the apparently simple question: Who causes the processing?

➜ Who takes the decision to process personal data and decides how and why, is the ©.

Examples of ©s

- A hotel with regard to its guests
- An association with regard to its members
- A clinic with regard to its patients
- Any company with regard to its employees
- A government with regard to the census

Decisions typically taken by a ©

- To create the company that needs to process data
- To define which data shall be processed
- To determine how they will be used
- To decide how long they will be kept
- To choose who can access them
- To engage another company to process them

Joint controllers

Where two or more © jointly determine the purposes and means of processing, they shall be joint controllers.

The processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.

Joint controllers

They shall determine their respective responsibilities for compliance with the obligations under GDPR by means of an arrangement between them.

➜ The essence of the arrangement shall be made available to the data subject.

➜ Data subjects may exercise their rights in respect of and against each of the joint ©s.

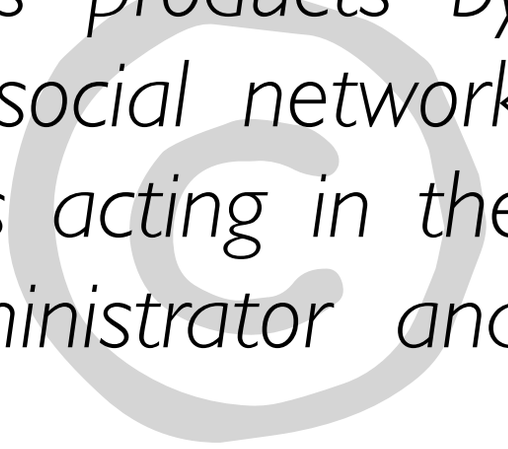
Some resolutions

The CJEU, in its judgment C-25/171, considered a religious community (Jehovah's Witnesses), together with the preaching members, as a data ©, with regard to the collection of personal data in connection with the door-to-door preaching activity.

Some resolutions

The CJEU, in judgment C-40/171, found that a website administrator who includes the Facebook Like button on the website is jointly responsible for the processing together with Facebook.

"*It allows him to optimise advertising for his products by making them more visible on the Facebook social network when a user clicks on the button, and thus, is acting in the economic interest of both the website administrator and Facebook.*"



Joint controllers

However, the EDPB states that "*the use of a common infrastructure or data processing system does not in all cases imply that the parties are jointly responsible for the processing*".

Joint controllers

There is no joint responsibility, if the data ©s:

- use the data for their own purposes; or
- the processing is independent and can be carried out by one of the parties without the intervention of the other.

Joint controllers

Another series of cases where co-responsibility does not exist:

- Processing of employee salary data by the company and by the tax authorities (there is a communication of data).
- Processing on a shared database or common infrastructure, where each accessing entity independently determines its own purposes.

Joint controllers

Finally, the CJEU, in judgment C-210/16, states that it is not necessary for the responsibility of the co-responsible parties to be equivalent.

They may «*be involved at different stages of the processing and to different degrees, so that the level of responsibility of each of them must be assessed in the light of all the relevant circumstances of the particular case*».

The data processor

Definition of data processor

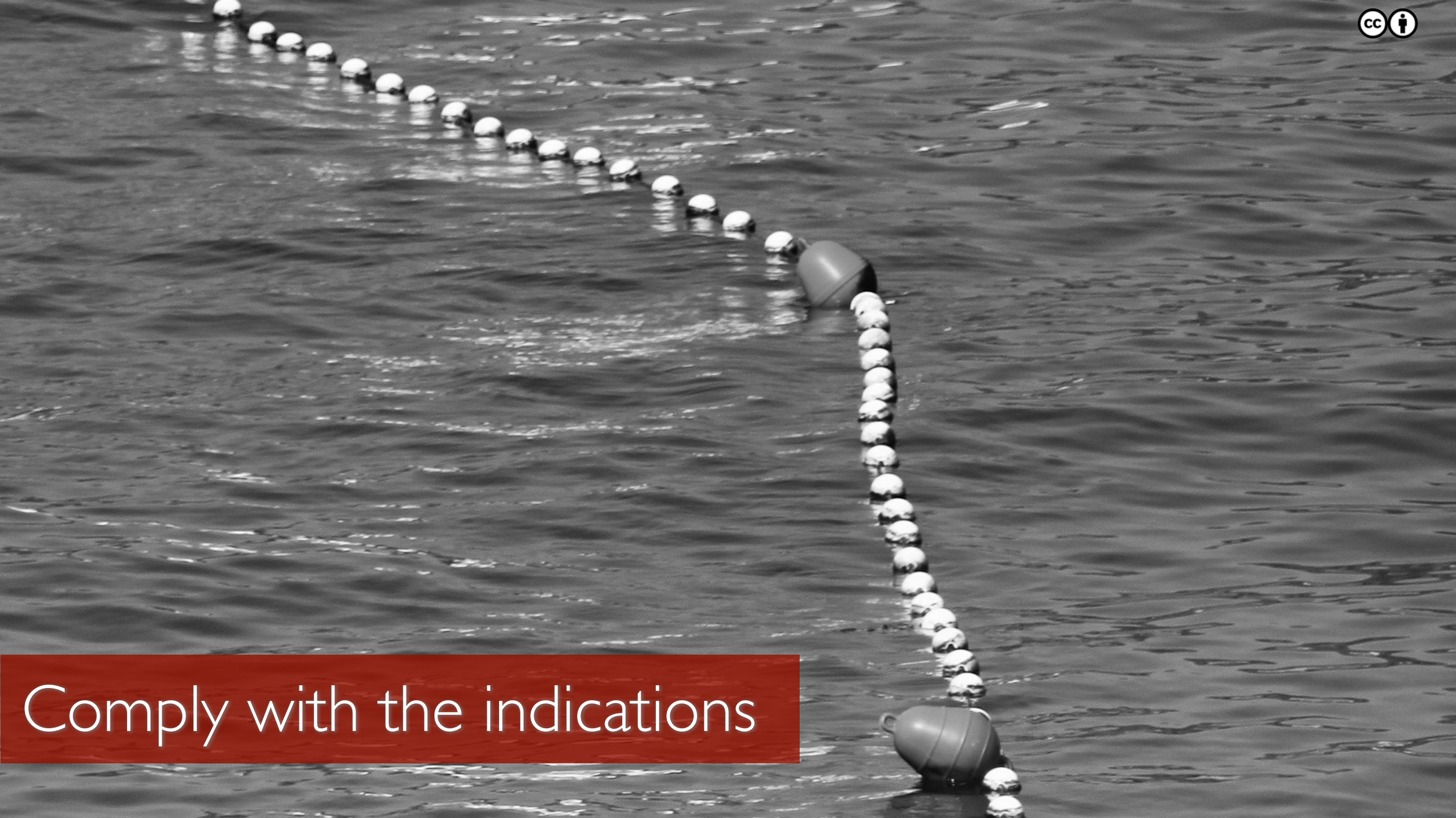
"The natural or legal person, public authority, agency or other body which processes personal data **on behalf of** the controller."

Art. 4.8) GDPR

Definition of data processor

Two basic conditions for qualifying as a Ⓟ are:

- It is a separate entity in relation to the Ⓒ;
- It processes personal data on the Ⓒ 's behalf.


Comply with the indications

The key factor: it acts on behalf of the ©

The Ⓟ is a natural or legal person, other than the ©, who processes personal data on its behalf.

While the © takes the decisions, the Ⓟ is subject to these decisions.

This concept was introduced to provide legal coverage to those service providers who need to access personal data.

The key factor: it acts on behalf of the ©

The EDPB explains that "*acting on behalf of*" means "*serving the interests of another and refers to the legal concept of delegation*".

So, the ©'s instructions may still leave a certain degree of discretion about how to best serve the ©'s interests.

The key factor: it acts on behalf of the ©

That's why the EDPB distinguishes between decisions on **essential means** (reserved to the ©) and decisions on **non-essential or technical means** (can be left to the discretion of the data Ⓟ).

Essential means

- Type of personal data processed: which data shall be processed?
- Duration of processing: for how long shall they be processed?
- Categories of recipients: who shall have access to them?
- Categories of data subjects: whose personal data are being processed?

Non-essential means

- More practical aspects of the processing such as:
  - the choice of a particular type of hardware or software; or
  - the decision on the details of security measures

Why does this concept exist?

It is designed to cover those delegated processing activities in which the Ⓟ must follow the instructions of the ©.

It is a legal fiction according to which the processing activities remain within the © 's organisation and, therefore, data are not formally disclosed to a third party, so no additional legal basis is needed.

Criteria for the correct interpretation

The Spanish Data Protection Agency (AEPD) indicates that this figure is necessary for those cases in which a company outsources services that implicitly involve the processing of data.

But qualifies that it is not necessary in all cases for the data processed to be owned by the data © (the processing operation commissioned may be directly the collection of the data).


The contract

The contract: an essential requirement

A contract between the © and the Ⓟ is required (art. 28 GDPR).

To start with, it must specify *"the subject-matter, the duration, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller"*.

Moreover, a Ⓟ must commit:

- To follow the documented instructions from the ©
- To establish internal obligations of confidentiality
- To implement appropriate security measures
- Not to subcontract without authorisation of the ©
- To assist the © if someone exercises his/her rights
- To assist the © regarding security and impact assessment
- To delete/return the data once the contract expires

What happens if the Ⓟ breaches the contract?

If the Ⓟ does not follow the instructions of the © (e.g., by processing data for its own purposes), it will be deemed to be another ©.

As a consequence, if the Ⓟ goes beyond the ©'s instructions:

- The legal fiction would fall
- Given the lack of legal basis, there would be a serious infringement of the GDPR

Things are what they are, and not what we want them to be

In any case, the concepts of © and Ⓟ are functional: they are based on the actual role performed by each party in the processing.

Therefore, the EDPB recalls that "*the legal status of the participants as* © *or* Ⓟ *should in principle be established by virtue of their concrete activities in a given situation and not on the basis of the formal designation (for example in a contract)*".

The © has *culpa in eligendo* and *culpa in vigilando* as regards the ℗ to which it delegates.

Culpa in eligendo and *culpa in vigilando*

The GDPR states that the © may only use Ⓟs providing sufficient guarantees to ensure that *"processing will meet the requirements"* of the GDPR.

It shall offer *"expert knowledge, reliability and resources"*.

How to deal with this responsibility?

It is crucial to engage only with companies providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of GDPR.

Moreover, the © has the obligation to monitor how the

Ⓟ complies with this Regulation, e.g. by conducting audits and inspections.


Accountability

How to deal with this responsibility?

The accountability principle is a central principle of GDPR and states that the © shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is in accordance with the GDPR.

It is directly addressed to the © but some of the more specific rules are addressed to both, © and Ⓟ.

"Legal principles and rules serve to highlight that not everything that is technically possible is also ethically admissible, socially acceptable, and legally approved."

STEFANO RODOTÀ

AUDENS

@maivaldeflores

maitane.valdecantos@audens.es

Abogacía Española
CONSEJO GENERAL

The project was funded by the European Union's Justice Programme (2014-2020)

ELF
EUROPEAN LAWYERS FOUNDATION

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Mercedes Ortuño Sierra

The Spanish data Protection Agency (AEPD)

Madrid, 15 February 2023

The project is co-financed with the support of the European Union's Justice programme

The Spanish data Protection Agency

Índex:

1. AEPD in a nutshell : Mission, Vision & Values
2. Legal Framework
3. AEPD Team, Tasks and Organisation
4. AEPD in Figures

1. AEPD in a Nutshell

Mission

Protecting persons in a digital world, particularly the most vulnerable groups. Strong commitment on social responsibility.

Fostering and **helping compliance** with data protection legislation, providing guidance (guide manuals and documents) and making available ad-hoc tools for private and public data controllers and processors.

Enforcing data protection **legislation**, developing investigations and managing complaints as required.

1. AEPD in a Nutshell

Vision

The AEPD wants to be the **centre of knowledge** on the lawful and fare processing of personal data, **supervising** the compliance with the GDPR; providing a **human face services** to individuals, useful **tools** for SMEs and **fostering ADR mechanisms**.

The AEPD wants to be a **key factor** for building the future **EU economy based on data**, **guiding on GDPR compliance** and on how to process personal data in a lawful, fare and ethical manner. AEPD wants to be the **guiding benchmark for technologic developments to come** (AI, internet of things, etc)

1. AEPD in a Nutshell

Values

- **Transparent** : AEPD is open and transparent in our actions and decision-making. Contracts, budget, salaries, and decisions are published.
- **Independent** : AEPD is independent from all external interests and impartial in its decision making.
- **Trustworthy**: AEPD´s decisions are legally and technically based, consistent and impartial. The security of confidential information are cornerstones of all our actions.
- **Efficient:** AEPD is results-oriented, committed and always seeking to use resources wisely. AEPD applies high quality standards and respect deadlines.
- **Socially Committed:** AEPD holds a “Social-Responsible Annual Plan” in favor of vulnerable groups, better governance, helping its human team and the environment (Special Reference to Priority Chanel)

2. The legal framework: the european factor

High level:

- Spanish Constitution 1978, article 18(4)
- **Regulation (EU) 2016/679 (GDPR)**

National Acts*:

- LO 5/1992 (LORTAD)
- LO 15/1999 (LOPD) (implementing Directive 95/46/CE)
- **LO 3/2018 (LOPDGDD)**
  - **Royal Decree 389/2021: AEPD Estatute**
- LO 1/2020 (on PNR, implementing Directive 2016/680)
- LO 7/2021 (on criminal issues, implementing Directive (EU) 2016/681)

*NB- Organic laws regulate fundamental rights

2. The legal framework: the constitutional mandate

Spanish Constitution, Article 18:

1. The right to honour, to **personal and family privacy** and to the own image is guaranteed.
4. The Law shall **restrict the use of data processing** in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.

- Constitutional Court, Ruling 292/2000:

  It explicitly recognizes the fundamental right to the protection of personal data as an independent right.

2. The legal framework: the highest legal rank

The Spanish data protection framework:

- **Regulation (EU) 679/2016 (GDPR)**
- **LO 3/2018 (LOPDGDD) (Organic Law or Constitutional Act)**
    - **Royal Decree 389/2021: AEPD Estatute**
- LO 1/2020 (implementing Directive 2016/281)
- LO 7/2021 (implementing Directive (EU) 2016/680)

3. AEPD Team, Tasks & Organisation

AEPD was established in 1994

Independent Supervisory Authority that monitors the observance of the data protection legal system.

- We guarantee and uphold the fundamental right to the protection of personal data.
- We act independently in exercising the functions entrusted to us (Director´s decisions can only be challenged at Courts)

3. AEPD Team, Tasks & Organisation

Tasks (Art 57 GDPR):

- Informing citizens and protecting their rights (active-reactive enforcement)
- Managing and deciding on complaints
- Consultation on legislation DP related
- Cooperating with DPOs
- Facilitating law´s implementation
- Identify and address new challenges
- Responding to the international dimension of Data Protection

3. AEPD Team, Tasks & Organisation

Independent way of working

Article 44 (LO 3/2018): General provisions.

1. The Spanish Data Protection Agency is an **independent administrative authority** at the state level, as provided for in Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, **with legal personality and full public and private capacity**, which **acts with full independence from the public authorities in the exercise of its functions**.

Its official name, in accordance with the provisions of Article 109.3 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, shall be "Agencia Española de Protección de Datos, Autoridad Administrativa Independiente" (***Spanish Data Protection Agency, Independent Administrative Authority***).

It liaises with the Government through the Ministry of Justice.

3. AEPD Team, Tasks & Organisation

Article 48: The Presidency of the Spanish Data Protection Agency

2. …shall exercise their functions with **full independence** and objectivity and shall **not be subject to any instruction** in the performance of their duties….

3. …shall be **appointed by the Government**, at the proposal of the Ministry of Justice, from among persons of **recognized professional** competence, particularly in the field of data protection. …after a **public call for candidates**…assessing the **merit, ability, competence** of the candidates… and the **approval of the Parliament** after a **hearing** (3/5 first round of ½ second round of >= 2 political groups).

In particular, it must be competent in the field of data protection (RD 389/2021, Art.12)

3. AEPD Team, Tasks & Organisation

Article 56: Foreign action

1.- AEPD is responsible for and **exercise of the functions** relating to the **foreign action of the State** in matters of **data protection…**

2. AEPD is the **competent body** for the protection of natural persons with regard to the processing of personal data deriving from the **application of any International Convention to which the Kingdom of Spain is a party** that confers on a national supervisory authority such competence and the common representative of the Data Protection authorities in the European Data Protection Board

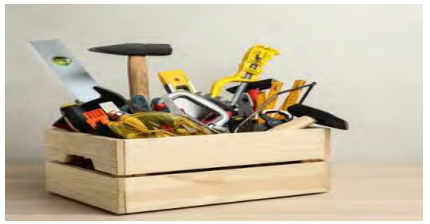
3. AEPD Team, Tasks & Organisation

Foreign action, in particular

- AEPD is member of the EDPB, on behalf of Spain
- Representative party at in the Global Privacy Assembly
- Founder (2003) and permanent Secretariat of the Iberoamerican DP Network
- Representative party at the Council of Europe for DP ad-hoc meetings and committees (Convention 108 and prospective Artificial intelligence Convention)

3. AEPD Team, Tasks & Organisation

7 hints for lawyers!!!



1.- Read carefully the AEPD´s Annual Report

(https://www.aepd.es/es/la-agencia/transparencia/informacion-economica-presupuestaria-y-estadistica/memorias)

2.- Use the Agency´s free tools for data controllers and processors (FACILITA, GESTIONA, etc)
https://www.aepd.es/es/guias-y-herramientas/herramientas

3.- Check the Guidance Documents (online guides on every DP related matter drafted the best in-house experts)
https://www.aepd.es/es/guias-y herramientas/guias?buscador_guias=&sort_bef_combine=field_advertise_on%20DESC&sort_by=field_advertise_on&sort_order=DESC&page=1

4.- FAQs: https://www.aepd.es/es/preguntas-frecuentes

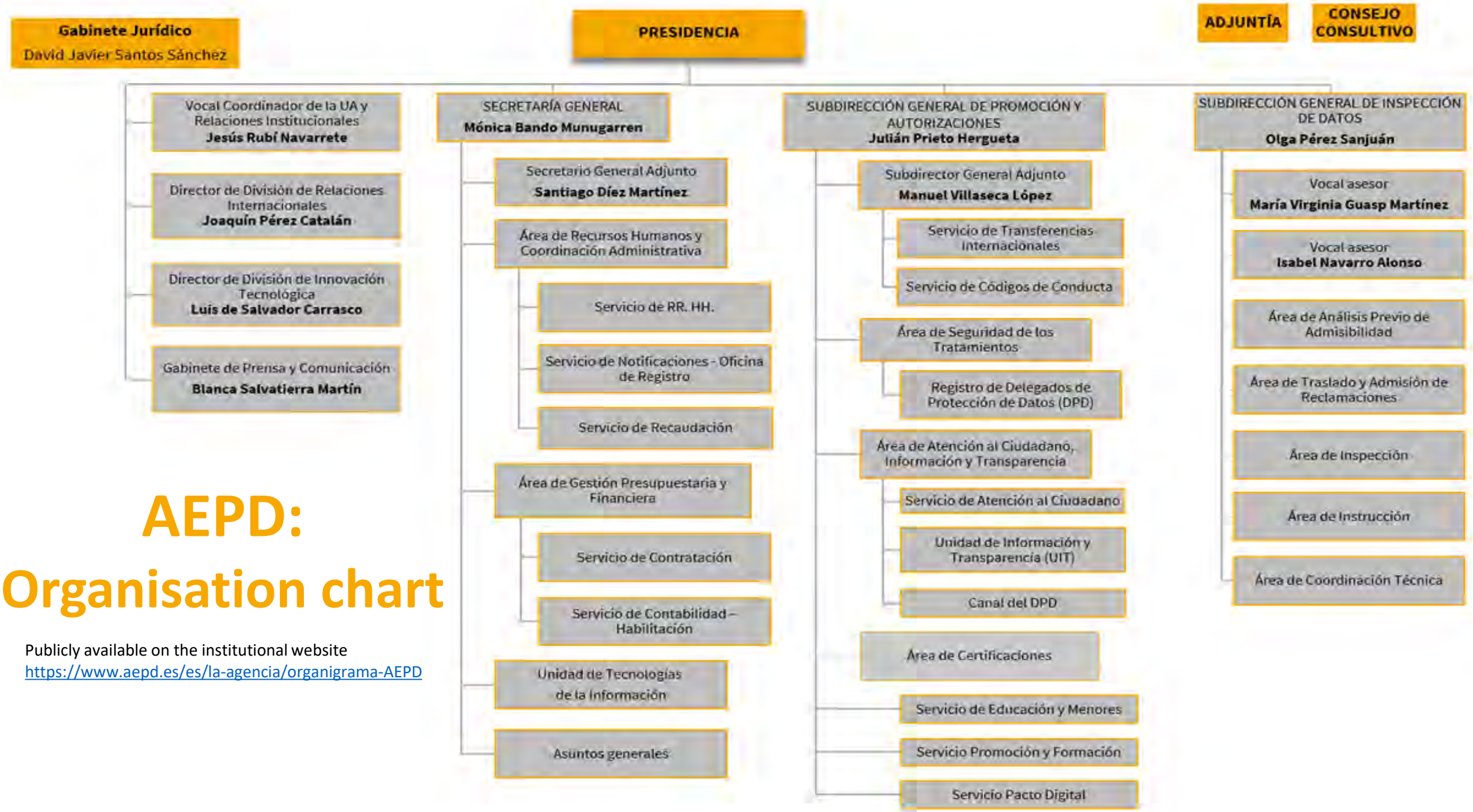
5.- Inquiry Channel for DPOs : https://www.aepd.es/es/guias-y-herramientas/herramientas/canalDPD

6.- AEPD´s Legal Reports : https://www.aepd.es/es/informes-y-resoluciones/informes-juridicos

7.- EDPB web site : https://edpb.europa.eu/edpb_en

AEPD:
Organisation chart

Publicly available on the institutional website
https://www.aepd.es/es/la-agencia/organigrama-AEPD



4. AEPD in Figures

COMPLAINTS

Issues to be managed	2021	2022	△ % Anual	% Relativo
Complaints submitted before the AEPD	13.905	15.128	9%	96%
Cross- border complaints	581	651	12%	4%
Ex Officio investigations	9	29	222%	0%
Follow up investigations triggered by data-breaches notified	76	14	-82%	0%
TOTAL	**14.571**	**15.822**	**9%**	**100%**

4. AEPD in Figures

DECISIONS

DECISION RATES	2021	2022	△% Anual	
Complaints decided per year	14.098	14.937	6%	
Pending Complaints	3.516	3.707	5%	
Rate of decided complaints vs lodged complaints	101%	99%	-2%	

4. AEPD in Figures

HELP DESK, GUIDANCE AND TOOLS

- 3.766 written inquires responded in 2022
- 42.562 phone inquiries attended
- 692 DPOs written inquiries attended
- 73 Guidance Manuals online
- Full set of IT-tools for lawful personal data processing and risk impact assessment (FACILITA, GESTIONA, etc.) online
- Comprehensive set of FAQs online
- Sectorial training and conferences: University and Schools; Public Sector DPOs; Health Sector DPOs; Tourism and hotels´DPOs
- Looking Forward: ChatBot in progress, tools for SMEs and Third Sector

4. AEPD in Figures

HHRR Figures

- 184 staff members
- 95% high qualified and experienced public officials (telecommunications engineers, IT experts, lawyers, attorneys, economists, journalists, administrators). 57% women
- Objectives and goals annual working program, audited regularly by external auditors
- Call center attended 100% by disabled (blind) experts on DP
- In-house training annual program
- Reclassification program
- Family and working life reconciliation program
- Well-being internal program (helping stress resilience & personal balance)

Muchas gracias for your attention!!!

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Michał Woźniak

Remedies, liability and penalties in GDPR

Madrid, 15 February 2023

The project is co-financed with the support of the European Union's Justice programme

Introduction

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Regulation 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 (hereinafter referred to as: „**General Data Protection Regulation**" or „**GDPR**"):

- binding in its entirety and directly applicable in all Member States of the European Union,
- entry into force on the 24th of May 2016,
- applied from the 25th of May 2018

(art. 99 par. 1 and 2 of GDPR).

Introduction

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Chapter VIII of General Data Protection Regulation titled:

Remedies, liability and penalties

regulates various means of legal protection in order to:

- ensure effective and proper application of the Regulation,
- secure all other rights of each data subject granted by other provisions of the Regulation for example Rights of the data subject regulated in Chapter III,
- prevent an infringement of the Regulation.

Chapter VIII of GDPR

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

I. **Rights constructed as remedies**
II. **Penalties**
III. **Liability**
IV. **Suspension of proceeding,obligation to contact the court in the other Member State, declining jurisdiction**

Introduction

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Rights constructed as remedies:

1) the right to lodge a complaint to a supervisory authority,
2) the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning natural or legal person,
3) the right to an effective judicial remedy against a controller or processor,
4) the right to receive compensation from the controller or processor for the damage suffered,
5) the right to mandate a not-for-profit body, organisation or association to represent the data subject.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Introduction

Penalties for the infringement of GDPR:

a) Criminal penalties (not introduced by GDPR)

b) Administrative penalties (including administrative fines)

Point 149 of the Preamble of GDPR:

Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. **Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice**.

Introduction

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Administrative penalties for the infringement of GDPR:

a) Administrative penalties regulated in article 58 point 2 of the Regulation,

a) Administrative fines - in order to strengthen and harmonize administrative penalties for infringements of this Regulation - imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2)

Introduction

Administrative penalties - article 58 point 2 of GDPR:

Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organization.

Introduction

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Administrative fines in GDPR - 2 exemplary, general divisions:

1. **Depending on the case of application**:

a) Imposed in case of non-compliance with an order by the supervisory authority as referred to in Article 58(2),

b) imposed instead of measures referred to in points (a) to (h) and (j) of Article 58(2),

c) imposed in addition to measure referred to in points (a) to (h) and (j) of Article 58(2),

2. **Depending on the upper limit of the fine**:

- up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (**does not regard the case of non-compliance with an order by the supervisory authority as referred to in Article 58(2)**);
- up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Introduction

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Liability – division on the type of the law establishing grounds and regulating the rules:

- Criminal liability (only mentioned in GDPR)
- Administrative liability (for example regulated in art. 83)
- Civil liability (the right to compensation resulting from an infringement of this Regulation)

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

I.
5 rights constructed as remedies

Right to lodge a complaint with a supervisory authority

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Article 77 of GDPR:

1.Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Right to an effective judicial remedy against a supervisory authority

Article 78 of GDPR:

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

Right to an effective judicial remedy against a supervisory authority

Article 78 par. 3 - 4 of GDPR:

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4.Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Right to an effective judicial remedy against a controller or processor

Article 79 of GDPR:

1.Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Right to mandate a not-for-profit body, organisation or association to represent the data subject

Article 80 of GDPR:

1.The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2.Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Right to compensation

Article 82 par. 1 and 6 of GDPR:

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

II. Administrative fines

Administrative fines – general assumptions

Point 150 of the Preamble of GDPR (an excerpt):

In order to strengthen and harmonize administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement.

Administrative fines – general conditions for imposing

Article 83 par. 1 of GDPR:

Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be **effective, proportionate and dissuasive**.

Administrative fines – general conditions for imposing

Article 83 par. 2 of GDPR (first sentence):

Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2).

Administrative fines – decisive criteria

Article 83 par. 2 of GDPR (second sentence):

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

Administrative fines – decisive criteria

Article 83 par. 2 of GDPR:

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Administrative fines – additional provisions

Article 83 par. 3, 7, 8, 9 of GDPR:

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

7.Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8.The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9.Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Administrative fines for essential infringement

Article 83 par. 5 letters a)-c) of GDPR:

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

Administrative fines for essential infringement

Article 83 par. 5 letters d)-e) of GDPR:

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

Administrative fines for essential infringement

Article 83 par. 6 of GDPR:

Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Administrative fines for other infringements

Article 83 par. 4 of GDPR:

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

II.

Other penalties with application of the rules on administration fines

Other penalties

Article 84 par. 1 and 2 of GDPR:

1.Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2.Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Other penalties with application of the rules on administration fines

Point 151 of the Preamble of GDPR:

The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

III. Liability

Liability

Article 82 par. 2 - 3 of GDPR:

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

Liability

Article 82 par. 4 - 5 of GDPR:

4.Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5.Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

Liability – point 146 of the Preamble of GDPR

The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law.

Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

IV.

Suspension of proceedings, obligation to contact the court in the other Member State, declining jurisdiction

Article 81 par. 1 - 3 of GDPR:

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

IV. Conclusions

1. The rights constructed as remedies require active performance of the entitled entity.

2. The institution of administration fines is a powerful sanction for the breach of GDPR and therefore prevention to avoid infringement is essential.

3. The right to compensation requires general prerequisites of liability for a damage to be fulfilled.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Thank You !

Michal Wozniak

attorney-at-law (Rz-K-290), Poland

michal.wozniak@gotfryd.pl

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Miguel Recio

Rights of the data subject, including rights in criminal investigations and proceedings

Madrid, 15 February 2023

The project is co-financed with the support of the European Union's Justice programme

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Content

- Charter of Fundamental Rights of the European Union.
- Data subjects´ rights in the GDPR.
- Restrictions or limitations.
- Data subjects rights in the Law Enforcement Directive (LED).
- Other relevant issues on data subjects´ rights.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Charter of Fundamental Rights of the European Union

Charter of Fundamental Rights of the European Union

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

"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."

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Data subjects´ rights in the GDPR

List of data subject´s rights in the GDPR

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Right of access by the data subject (Art. 15)
- Right to rectification (Art. 16)
- Right to erasure ('right to be forgotten') (Art. 17)
- Right to restriction of processing (Art. 18)
- Right to data portability (Art. 20)
- Right to object (Art. 21)
- Automated individual decision-making, including profiling (Art. 22)
- Right to withdraw consent (Art. 13(2)(c))
- Right to lodge a complaint with a supervisory authority (Art. 13(2)(d))

Right of access by the data subject

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- To obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.
- If data subject´s personal data are processed:
  - Access to personal data.
  - Information on the processing.
- The right to obtain a copy of the personal data processed shall not adversely affect the rights and freedoms of others (Art. 15(4)).

Right of access by the data subject

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Judgment of the Court (First Chamber), 12 January 2023, in case C-154/21. Ruling: "Article 15(1)(c) of 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), must be interpreted as meaning that the data subject's right of access to the personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the actual identity of those recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of Regulation 2016/679, in which cases the controller may indicate to the data subject only the categories of recipient in question".
- Consulted at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=269146&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=368828

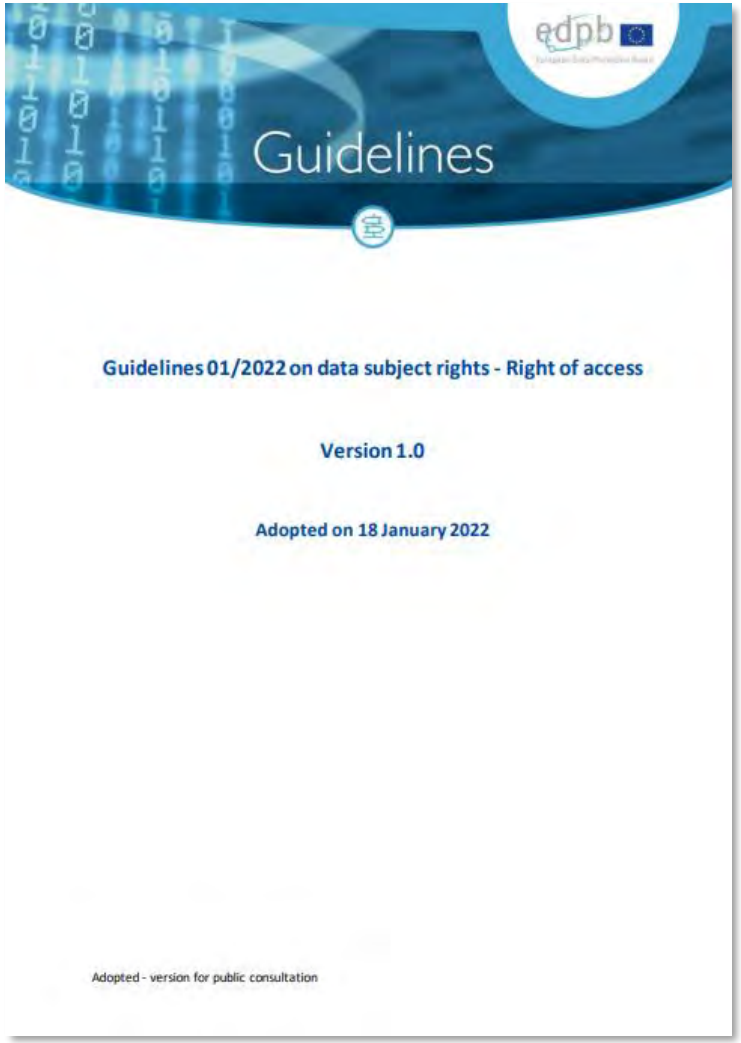
Right of access by the data subject

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Judgment of the Court (Second Chamber), 20 December 2017, in case C-434/16. Ruling: "Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as meaning that, in circumstances such as those of the main proceedings, the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data, within the meaning of that provision".
- Consulted at: https://curia.europa.eu/juris/document/document.jsf?docid=198059&doclang=EN

Guidelines of the EDPB



Guidelines 01/2022 on data subject rights - Right of access

Consulted at: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Right to rectification

- Rectification of inaccurate personal data concerning the data subject.
- To have personal data completed taking into account the purposes of the processing.
- Without undue delay.

Right to erasure ('right to be forgotten') - Grounds

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- General rule: erasure of personal data concerning the data subject without undue delay (Art. 17(1)).
- Where one of the following grounds applies:
  - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (Art. 17(1)(a));
  - the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing (Art. 17(1)(b));
  - the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) (Art. 17(1)(c));
  - the personal data have been unlawfully processed (Art. 17(1)(d));
  - the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject (Art. 17(1)(e));
  - the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) (Art. 17(1)(f)).

Right to erasure ('right to be forgotten') - Exceptions

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- It shall not apply not apply to the extent that processing is necessary:
  - for exercising the right of freedom of expression and information (Art. 17(3)(a));
  - for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 17(3)(b))
  - for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) (Art. 17(3)(c))
  - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing (Art. 17(3)(d)); or
  - for the establishment, exercise or defence of legal claims (Art. 17(3)(e)).

Right to be forgotten

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Judgment of the Court (Grand Chamber), 13 May 2014, in case C-131/12. Ruling: "Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d). […]".
- Consulted at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=377631

Right to be forgotten

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Judgment of the Court (Grand Chamber), 24 September 2019, in case C-507/17. Ruling: "On a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and of Article 17(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation), where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request" (territorial scope of the right to de-referencing).
- Consulted at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=372984

Right to be forgotten

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Judgment of the Court (Grand Chamber), 8 December 2022, in case C-460/20. Ruling: "Article 17(3)(a) of 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), must be interpreted as meaning that within the context of the weighing-up exercise which is to be undertaken between the rights referred to in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, on the one hand, and those referred to in Article 11 of the Charter of Fundamental Rights, on the other hand, for the purposes of examining a request for de-referencing made to the operator of a search engine seeking the removal of a link to content containing claims which the person who submitted the request regards as inaccurate from the list of search results, that de-referencing is not subject to the condition that the question of the accuracy of the referenced content has been resolved, at least provisionally, in an action brought by that person against the content provider" (Dereferencing of allegedly inaccurate content).

- Consulted at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=268429&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=375061

Right to restriction of processing

Where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data (Art. 18(1)(a));
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead (Art. 18(1)(b));
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims (Art. 18(1)(c));
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject (Art. 18(1)(d)).

Right to restriction of processing

- Personal data shall, with the exception of storage, only be processed:
  - with the data subject's consent or
  - for the establishment, exercise or defence of legal claims or
  - for the protection of the rights of another natural or legal person or
  - for reasons of important public interest of the Union or of a Member State (Art. 18(2)).

- The data subject shall be informed by the controller before the restriction of processing is lifted (Art. 18(3)).

Notification obligation regarding rectification or erasure of personal data or restriction of processing

- Obligation to communicate by the controller.
- To each recipient to whom the personal data have been disclosed.
- Unless this:
  - proves impossible or
  - involves disproportionate effort.
- The controller shall inform the data subject about those recipients if the data subject requests it.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Right to data portability

- The right to receive the personal data concerning [the data subject],
  - which he or she has provided to a controller,
  - in a structured, commonly used and machine-readable format and

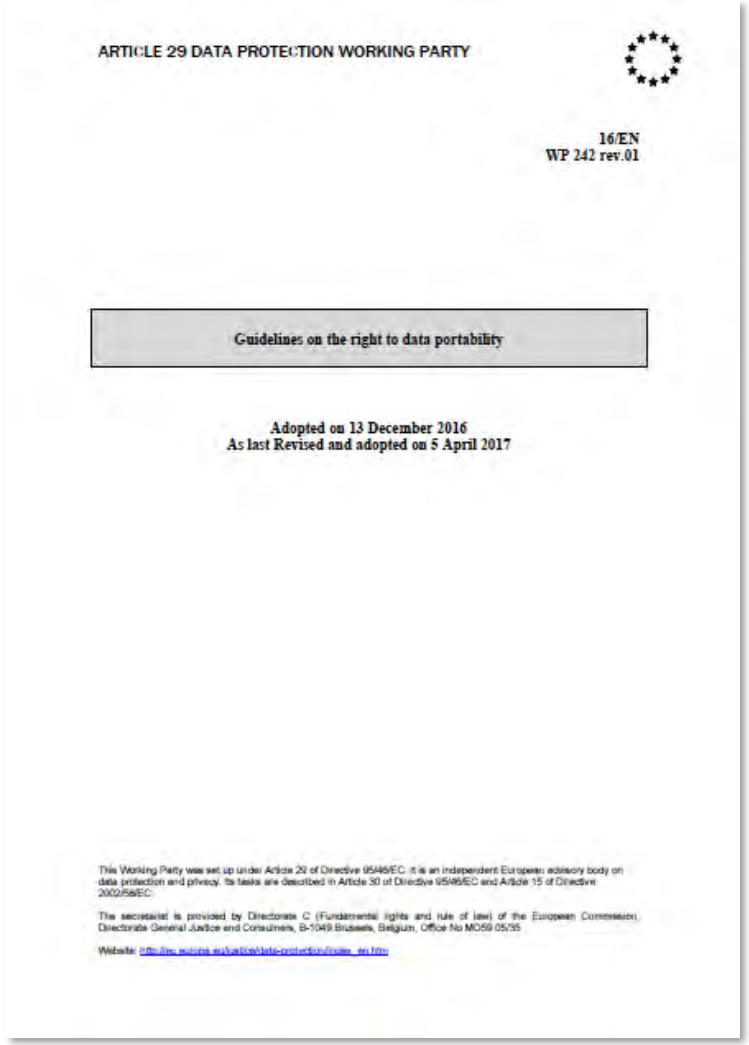
- The right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided" (Art. 20(1)).
- Where the processing is:
  - based on consent (Arts. 6(1)(a) or 9(1)(a)) or on a contract (Art. 6(1)(b));
  - Carried out by automated means.

- It shall not adversely affect the rights and freedoms of others.

Guidelines of the EDPB

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2



ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 242 rev.01

Guidelines on the right to data portability

Adopted on 13 December 2016
As last Revised and adopted on 5 April 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 rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

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

A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":

- **Data actively and knowingly provided by the data subject** (for example, mailing address, user name, age, etc.)
- **Observed data provided by the data subject by virtue of the use of the service or the device**. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.

In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". For example, the outcome of an assessment regarding the

Consulted at:
https://ec.europa.eu/newsroom/article29/items/611233/en

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Right to object

- The data subject can object to processing (including profiling), on grounds relating to his or her particular situation (Art. 21(1)).
- Controllers are specifically required to provide for this right in all cases where processing is based on Article 6(1) (e) or (f).
- The controller must interrupt (or avoid starting) the profiling process unless it can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the data subject.
- The controller may also have to erase the relevant personal data,
- Unconditional (no need for any balancing of interests) right to object to the processing of their personal data for direct marketing purposes, including profiling to the extent that it is related to such direct marketing (Art. 21(2)).

EDPB, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). Consulted at: https://ec.europa.eu/newsroom/article29/items/612053/en

Automated individual decision-making, including profiling

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- 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 the data subject.
- It shall not apply if the decision is:
  - necessary for entering into, or performance of, a contract between the data subject and a data controller
  - 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
  - based on the data subject's explicit consent.
- Right to obtain human intervention on the part of the controller (contract or explicit consent), to express the data subject point of view and to contest the decision.
- Decision shall not be based on special categories of personal data, 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.

Automated individual decision-making, including profiling

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- "The term "right" in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing."

EDPB, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). Consulted at: https://ec.europa.eu/newsroom/article29/items/612053/en

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Right to withdraw consent

- When consent is the legal basis for the processing of personal data.
- At any time.
- Without affecting the lawfulness of processing based on consent before its withdrawal.

Right to lodge a complaint with a supervisory authority

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- If the data subject considers that the processing of personal data relating to him or her infringes the GDPR (Art. 77(1)).
- In particular in the Member State of his or her:
  - habitual residence,
  - place of work or
  - place of the alleged infringement
- The Supervisory Authority (SA) shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy (Art. 77(2)).
- List of SAs: https://edpb.europa.eu/about-edpb/about-edpb/members_en

Transparent information, communication and modalities for the exercise of the rights of the data subject

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

The controller shall:

- Take appropriate measures to provide any communication under Articles 15 to 22 (Art. 12(1)).
- In a concise, transparent, intelligible and easily accessible form.
- Provide information on action taken on a request without undue delay (Art. 12(3)):
  - In any event within one month of receipt of the request
  - That period may be extended by two further months where necessary complexity and number of the requests
- The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Transparent information, communication and modalities for the exercise of the rights of the data subject

- The controller shall:
  - inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (Art. 12(4)).
- Any communication and any actions taken shall be provided free of charge (Art. 12(5)).
- Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
  - (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
  - (b) refuse to act on the request.

Transparent information, communication and modalities for the exercise of the rights of the data subject

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject (Art. 12(6)).

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Restrictions

Requirements under Article 23(1) GDPR

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

i. Respect of the essence of the fundamental rights and freedoms;

ii. Proportionality and necessity test;

iii. Legislative measures laying down restrictions and the need to be foreseeable (Recital 41 and CJEU case law);

iv. Data subjects' rights and controller's obligations which may be restricted, and

v. Grounds for the restrictions.

Requirements under Article 23(2) GDPR

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

i. The purposes of the processing or categories of processing;

ii. The categories of personal data;

iii. The scope of the restrictions introduced;

iv. The safeguards to prevent abuse or unlawful access or transfer;

v. The specification of the controller or categories of controllers;

vi. The storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

vii. The risks to the rights and freedoms of data subjects, and

viii. The right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Guidelines and recommendations of the EDPB

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Guidelines 10/2020 on restrictions under Article 23 GDPR
  - Consulted at: https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf

- Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive
  - Consulted at: https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf

Enforcement of civil law claims

While Article 23(1)(j) GDPR allows limitations to protect the individual interests of a (potential) litigant, Article 23(1)(f) GDPR allows limitations to protect the court proceedings themselves as well as the applicable procedural rules:

- The enforcement of civil claims (Article 23(1)(j) GDPR).
- The protection of judicial independence and judicial proceedings.

Restriction to access in criminal matters

- In certain cases, providing information to the data subjects who are under investigation might jeopardise the success of that investigation.
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Article 23(1)(d) GDPR).
- The protection of the data subject or the rights and freedoms of others (Article 23(1)(i) GDPR).

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Data subjects´ rights in the Law Enforcement Directive (LED)

(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)

List of data subject´s rights in the LED

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Information to be made available or given to the data subject (Art. 13).
- Right of access by the data subject (Art. 14).
- Limitations to the right of access (Art. 15).
- Right to rectification or erasure of personal data and restriction of processing (Art. 16).
- Rights of the data subject in criminal investigations and proceedings (Art. 17).
- Right to lodge a complaint with a supervisory authority (Art. 52),

Right of access

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- The right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.
- Access to the personal data.
- The following information:
  - the purposes of and legal basis for the processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;
  - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
  - the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;
  - the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;
  - communication of the personal data undergoing processing and of any available information as to their origin.

Limitations to the right of access (I)

- Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access
- To the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:
  - avoid obstructing official or legal inquiries, investigations or procedures (Art. 15(1)(a));
  - avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties (Art. 15(1)(b));
  - protect public security (Art. 16(4)(c));
  - protect national security (Art. 15(1)(d));
  - protect the rights and freedoms of others (Art. 15(1)(e)).
- Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under previous points ((a) to (e)).

Limitations to the right of access (II)

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- The controller shall inform to the data subject of:
  - any refusal or restriction of access and of the reasons for the refusal or the restriction.
    - without undue delay,
    - in writing
    - such information may be omitted where the provision thereof would undermine a purpose under Article 15(1).
  - the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

Restrictions to the rights to rectification or erasure of personal data and restriction of processing

- If restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:
  - avoid obstructing official or legal inquiries, investigations or procedures (Art. 16(4)(a));
  - avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties (Art. 16(4)(b));
  - protect public security (Art. 16(4)(c));
  - protect national security (Art. 16(4)(d));
  - protect the rights and freedoms of others (Art. 16(4)(e)).
- The controller shall inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy (last paragraph of Art. 16(4)).

Rights of the data subject in criminal investigations and proceedings

- Member States may provide for the exercise of the rights of:
  - of information to be made available or given to the data subject,
  - of access,
  - to rectification or erasure of personal data and restriction of processing
- to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Other relevant issues on data subjects´ rights

Powers of Supervisory Authorities (SAs)

If corrective measures need to be applied, the SAs can in accordance with Article 58(2) GDPR order:

- the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to the GDPR;
- the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 GDPR and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19 GDPR.

Infringements and fines in the GDPR

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Infringement of the data subjects' rights pursuant to Articles 12 to 22:
  - Administrative fines up to 10.000.000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

- Non-compliance with an order by the SA authority as referred to in Article 58(2):
  - Administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Penalties in the LED

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive (Art. 84(1)).

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Thank you!

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Paula Ortiz López

Interplay between GDPR and e-Privacy

Madrid, 15 February 2023

The project is co-financed with the support of the European Union's Justice programme

Agenda

1. Context. Digital enviroment
2. GDPR and digital enviroment
3. E-privacy regulation
4. Interplay between GDPR & e-Privacy
5. Cookies and id´s. European scope

GDPR Data Protection

personal data' means 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;

SCOPE OF APPLICATION

PRINCIPLES

RIGHTS

E-Privacy

- Prohibition of comercial communications without explicit consent
- Obligation to identify comercial comunications
- Role of cookies

Privacy and Data Protection. From this….

HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

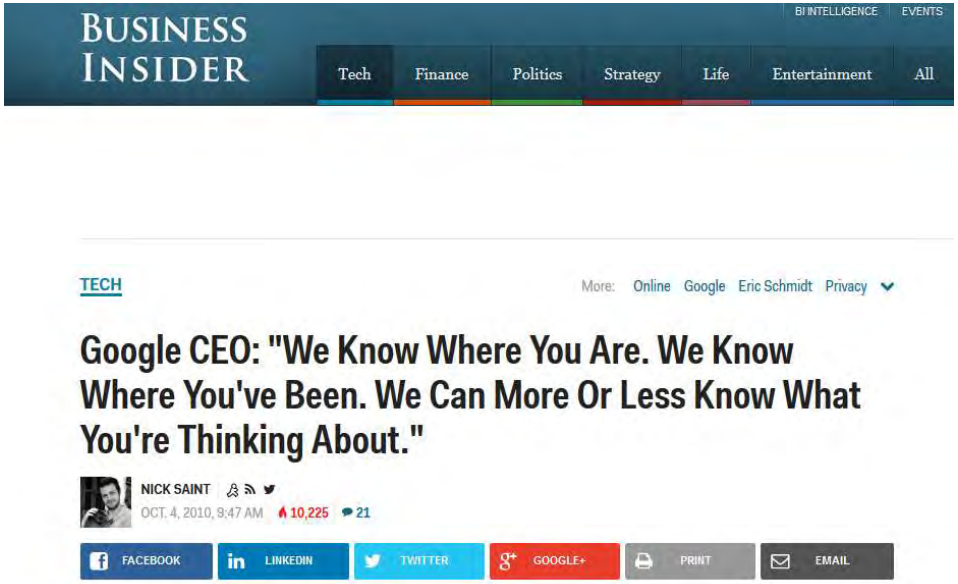
WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession — intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in

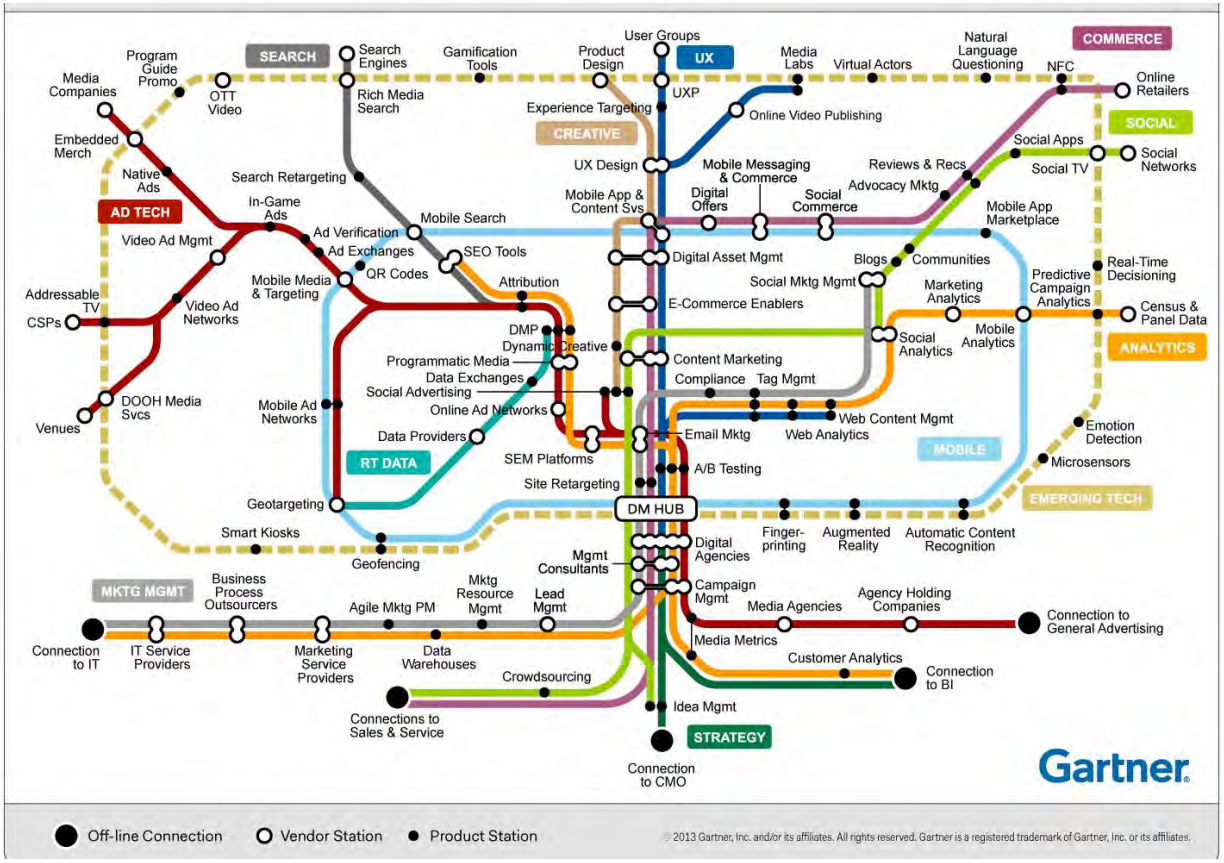
the right "to be let alone."

To this…


BUSINESS INSIDER
BI INTELLIGENCE
EVENTS
Tech
Finance
Politics
Strategy
Life
Entertainment
All
TECH
More:
Online
Google
Eric Schmidt
Privacy
Google CEO: "We Know Where You Are. We Know Where You've Been. We Can More Or Less Know What You're Thinking About."
NICK SAINT
OCT. 4, 2010, 9:47 AM
10,225
21
FACEBOOK
LINKEDIN
TWITTER
GOOGLE+
PRINT
EMAIL


THE NEW WAY TO CAPTURE, SHARE & LISTEN.
Ray-Ban
FACEBOOK
RAY-BAN STORIES

Sources of data in digital enviroment



First Party Data
Second party Data
Third Party Data
Cookies
Ids
Analytics…

Privacy in Europe

"The EU provides the right to have your personal data protected by strong, European laws…because in Europe privacy matters."

Jean-Claude Juncker, President of the European Commission
Brussels, 14 September 2016

GDPR and digital enviroment: A wide range of businesses affected:

-Measurement (currency of the internet)
-Web analytics
-Ad delivery and Ad targeting

Global application

Personal data
Ids Cookies, geolocalization, online identifiers, Ips, MAC Address

Pseudonimización

Consent
1.Freely given: The user must be giving consent of their own will. They weren't pressured into giving consent.
2.Specific: The user must be asked to consent to specific types of data processing.
3.Informed: The user must be told what they're consenting to.
4.Unambiguous: The language used in the cookie notice banner solution must be simple and clear.
5.Clear affirmative action: The user must clearly express consent by saying or doing something (e.g., clicking a button to agree).

Rigths of the data subject

Accountability
Privacy by design

Information

Data Protection Officer "(…)"

Privacy Impact Assesment

Fines
20 mill euros
4% global turnover

Profiling

GDPR and digital enviroment

- The GDPR represents a substantial milestone, establishing the data protection principles for the digital advertising sector.
- It has a comprehensive scope and guarantees the protection of personal data both in the context of electronic communications services and information society services.
- In fact, the GDPR unambiguously mentions pseudonymous identifiers (Rec. 26), online identifiers, cookies, and device identifiers as examples of personal data (Art. 4 (1), Recital 30).
- In addition, the GDPR contains rules on profiling, providing enhanced rights to users (Art. 4 (4), Art. 22, Recital 72), including where user behavior is tracked online (Recital 24).
- The GDPR also refers specifically to online advertising (Recital 58).
- In practice, the digital advertising ecosystem is based on processing data for advertising-related purposes, including but not limited to the delivery and measurement of digital advertising.
- The data processed may include IP addresses, online advertising identifiers, URLs of sites where users spend time, information about user behavior on those sites, and indications of the physical whereabouts of users ("geolocation" data).
- Most, or all, of this data is considered personal data under the GDPR. And therefore from this perspective, the GDPR is the main legal regime applicable to the advertising ecosystem. And more, perhaps, when the cookie system changes in the near future. But the potential of the GDPR to bring stability to the sector is reduced by the legal uncertainty caused by the ePrivacy proposal

Consent with GDPR

Article 4(11) GDPR defines“the consent of the data subject” as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

“ticking a box when visiting a... website, choosing technical settings... or by any other statement or conduct which clearly indicates... the data subject’s acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes or inactivity should therefore not constitute consent.

Explicit consent is still required to justify the processing of sensitive personal data (unless other grounds apply)

I agree (afirmative action))

Silence and pre checked boxes.

Consent with GDPR for marketing purposes

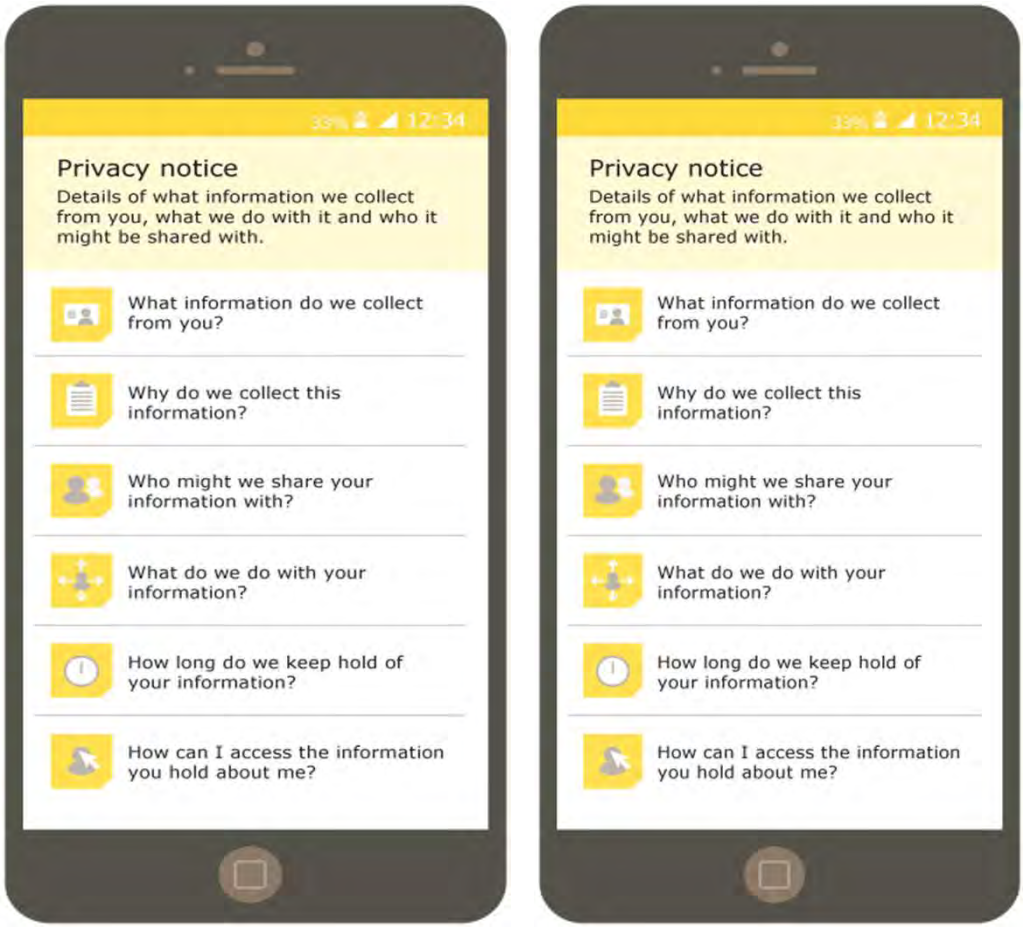
If the data subject's consent is given in the context of a written declaration which also concerns other matters, **the request for consent shall be presented in a manner which is clearly distinguishable from the other matters**, in an intelligible and easily accessible form, using clear and plain language.

- ☑ Accept Purpose 1
- ☑ Accept Purpose 2
- ☑ Accept Purpose 3

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4

Transparency with GDPR



How to provide it

We provide the information in a way that is:

☐ concise;
☐ transparent;
☐ intelligible;
☐ easily accessible; and
☐ uses clear and plain language.

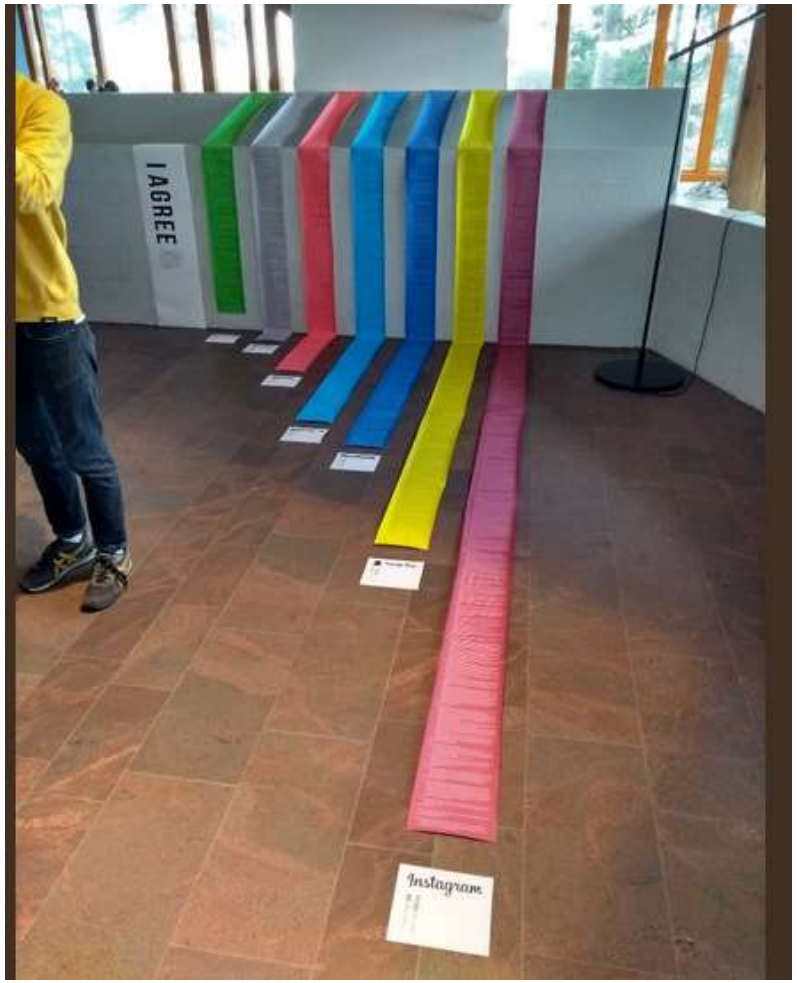
Best practice – delivering the information

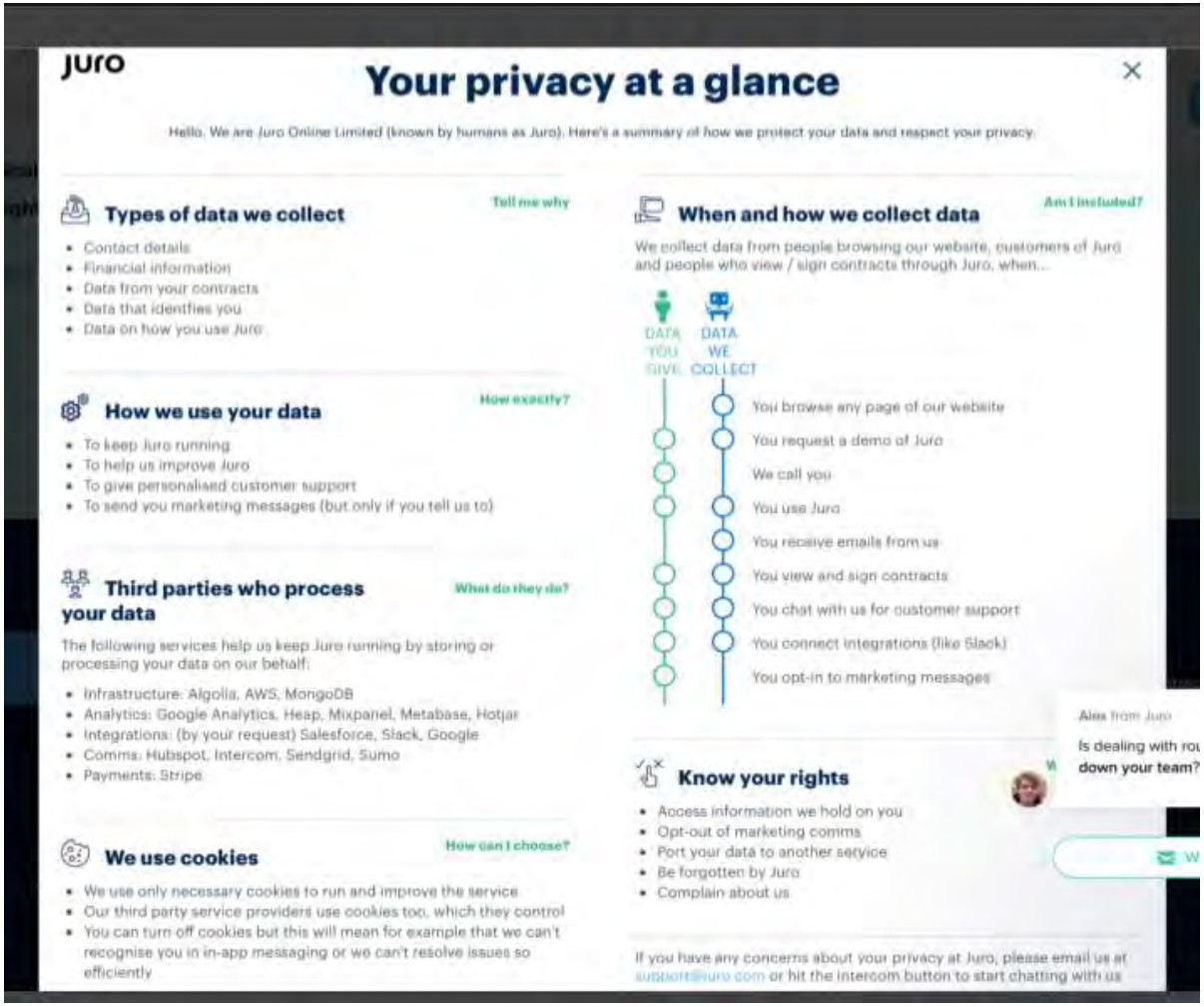
When providing privacy information to individuals, use a combination of appropriate techniques, such as:

☐ a layered approach;
☐ dashboards;
☐ just-in-time notices;
☐ icons; and
☐ mobile and smart device functionalities.

By placing an order via this web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions. We reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction.
Click here to nulify your soul transfer.


I AGREE.


I AGREE
Instagram

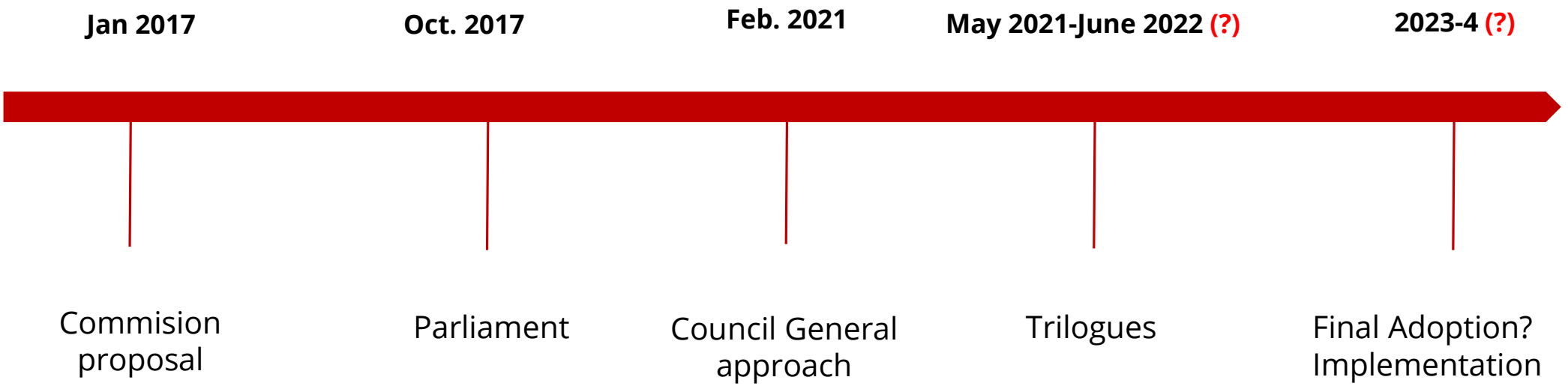

juro
Your privacy at a glance
Hello. We are Juro Online Limited (known by humans as Juro). Here's a summary of how we protect your data and respect your privacy.
Types of data we collect
Tell me why
Contact details
Financial information
Data from your contracts
Data that identifies you
Data on how you use Juro
How we use your data
How exactly?
To keep Juro running
To help us improve Juro
To give personalised customer support
To send you marketing messages (but only if you tell us to)
Third parties who process your data
What do they do?
The following services help us keep Juro running by storing or processing your data on our behalf:
Infrastructure: Algolia, AWS, MongoDB
Analytics: Google Analytics, Heap, Mixpanel, Metabase, Hotjar
Integrations: (by your request) Salesforce, Slack, Google
Comms: Hubspot, Intercom, Sendgrid, Sumo
Payments: Stripe
We use cookies
How can I choose?
We use only necessary cookies to run and improve the service
Our third party service providers use cookies too, which they control
You can turn off cookies but this will mean for example that we can't recognise you in in-app messaging or we can't resolve issues so efficiently
When and how we collect data
Am I included?
We collect data from people browsing our website, customers of Juro and people who view / sign contracts through Juro, when...
DATA YOU GIVE
DATA WE COLLECT
You browse any page of our website
You request a demo of Juro
We call you
You use Juro
You receive emails from us
You view and sign contracts
You chat with us for customer support
You connect integrations (like Slack)
You opt-in to marketing messages
Know your rights
Access information we hold on you
Opt-out of marketing comms
Port your data to another service
Be forgotten by Juro
Complain about us
If you have any concerns about your privacy at Juro, please email us at support@juro.com or hit the intercom button to start chatting with us
Alex from Juro
Is dealing with rou
down your team?

Profiling

- Profiling activities defined as those that “evaluate in particular a natural person’s performance at work, economic situation, location, health, personal preferences, reliability or **behaviou**r”.
- 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 unless:
    - (explicit) consent
    - entering into a contract

- Advertising doesn’t enter in this definition.

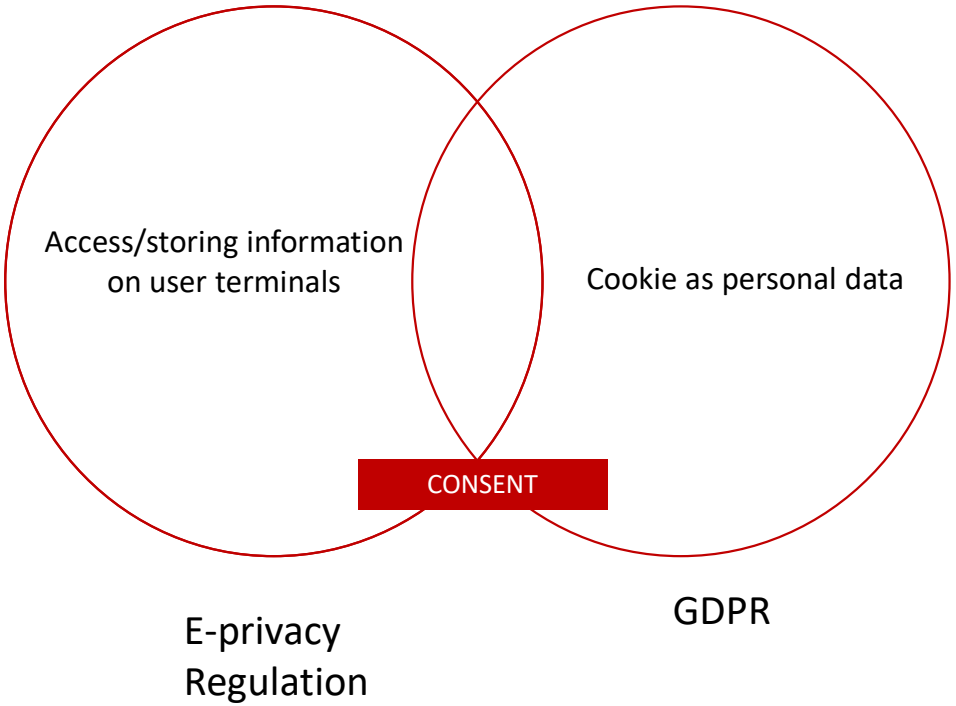
Timeline e-Privacy



Presidencia Eslovena. Enero 2022 Francia

e-Privacy- GDPR

- D 95/46 — D 2002/58
- GDPR — D 2009/136
- GDPR — e-Privacy regulation



- The interconnection between GDPR and e-Privacy has always been clear. Cross-references:
- Same competent authority
- Matters linked to both standards such as cookies or the relationship between service providers and users.
- Two standards that complement each other.
- It has been said that e-Privacy is necessary to reinforce the GDPR in specific aspects (privacy of communications, metadata, compatible purposes of processing...) But there are other issues in which it does not introduce reinforcement.
- The ePrivacy Regulation should not reduce the level of protection of the GDPR but should not limit it either.

Which law should apply?

E-Privacy sits alongside the GDPR, and provides specific rules in relation to privacy and electronic communications.

Where these rules apply, they take precedence over the GDPR.

With cookies you need to consider e-Privacy compliance first **before** you look to the GDPR.

Additionally, E-Privacy depends on data protection law for some of its definitions.

For example E-Privacy takes the GDPR's standard of consent. The GDPR also talks about cookies within the definition of personal data.

Essentially, if you are operating an online service, then the easiest way to look at the two laws is:

- if your online service stores information, or accesses information stored, on user devices then you should ensure that comply with E-Privacy first, including the requirements to provide information and obtain consent; and
- the GDPR applies to any processing of personal data outside of this storage or access.

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP259 rev.01

Article 29 Working Party
Guidelines on consent under Regulation 2016/679

Adopted on 28 November 2017
As last Revised and Adopted on 10 April 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE

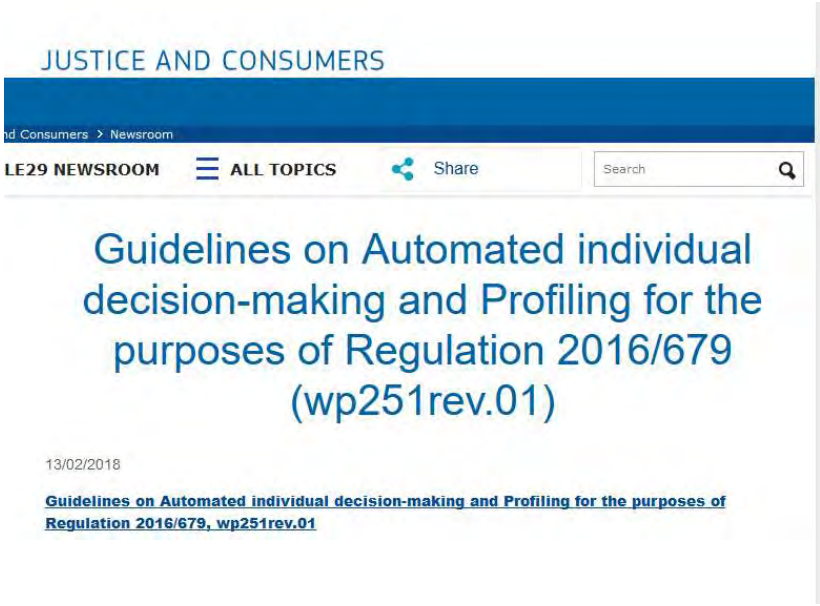
PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:



Directive 2002/58

Directive 2009/136

AD CHOICES

Advertising industry solution

Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities

Adopted on 12 March 2019

Does the mere fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limit the competences, tasks and powers of data protection authorities under the GDPR?

Data protection authorities are competent to enforce the GDPR.

The mere fact that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR.

Should infringements of national ePrivacy rules be set aside when in assessing compliance with the GDPR, and if so when?
The authority that are appointed as competent in the meaning of the ePrivacy Directive by Member States is exclusively responsible for enforcing the national provisions transposing the ePrivacy Directive that are applicable to that specific processing operation, including in cases where the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive. Nevertheless, data protection authorities remain fully competent as regards any processing operations performed upon personal data which are not subject to one or more specifics rules contained in the ePrivacy Directive.

An infringement of the GDPR might also constitute an infringement of national ePrivacy rules. The data protection authority may take this factual finding as to an infringement of ePrivacy rules into consideration when applying the GDPR (e.g., when assessing compliance with the lawfulness or fairness principle under article 5(1)a GDPR). However, any enforcement decision must be justified on the basis of the GDPR, unless the data protection authority has been granted additional competences by Member State law.
90. If national law designates the data protection authority as competent authority under the ePrivacy Directive, this data protection authority has the competence to directly enforce national ePrivacy rules in addition to the GDPR (otherwise it does not).

E-PRIVACY REGULATION. Parlament Proposal.

- Inambiguos consent
- Browsers must block all cookies
- Prohibition of cookie walls

Cookies

What are ‘cookies’?

Cookies are small pieces of information, normally consisting of just letters and numbers, which online services provide when users visit them. Software on the user's device (for example a web browser) can store cookies and send them back to the website next time they visit.

How are cookies used?

Cookies are a specific technology that store information between website visits. They are used in numerous ways, such as:

- remembering what’s in a shopping basket when shopping for goods online;
- supporting users to log in to a website;
- analysing traffic to a website; or
- tracking users' browsing behaviour.

Cookies can be useful because they allow a website to recognise a user’s device. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Without cookies, or some other similar method, websites would have no way to ‘remember’ anything about visitors, such as how many items are in a shopping basket or whether they are logged in.

Cookies

Depending on the website domain

- First Party
- Third Party

Depending on the time:

- Session
- Persistent

Depending on purpose:

- Technical
- Preferences/personalization
- Analytics & measurement
- Behavioral advertising

How to comply.

How do we plan and decide what type of cookies to use?

If you are planning a new online service, you should take steps to detail what cookies you will use, which are strictly necessary, and ensure that you have appropriate arrangements in place with any third parties. For any pre-existing services, you should already know what types of cookies you use but it would be sensible to recheck.

This might take the form of a comprehensive ‘cookie audit’ of your online service, or it could be as simple as checking what data will be sent to users and why.

How do we tell people about cookies?

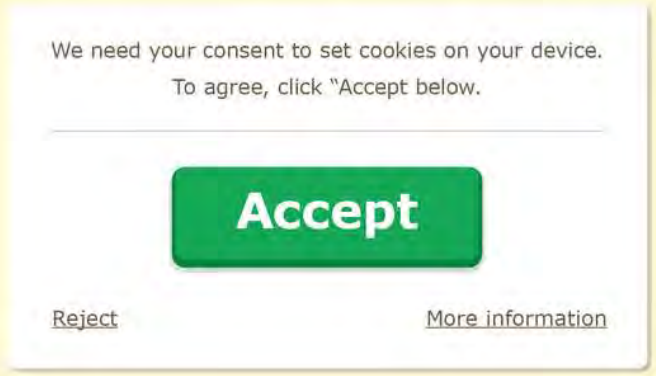
You also need to tell people about the purposes and duration of the cookies you use.
You need to provide information about cookies in such a way that the user will see it when they first visit your service.

You should also provide more detailed information about cookies in a privacy or cookie policy accessed through a link within the consent mechanism and at the top or bottom of your website.
Ultimately, users may be more likely to give their consent to non-essential cookies where they fully understand:
•what you use cookies for;
•how you have gone about seeking their consent;
•how you (and any third party) intends to use their data; and
•that you have provided them with appropriate control over their preferences.
This can also be a means of enhancing trust and confidence in your online service.

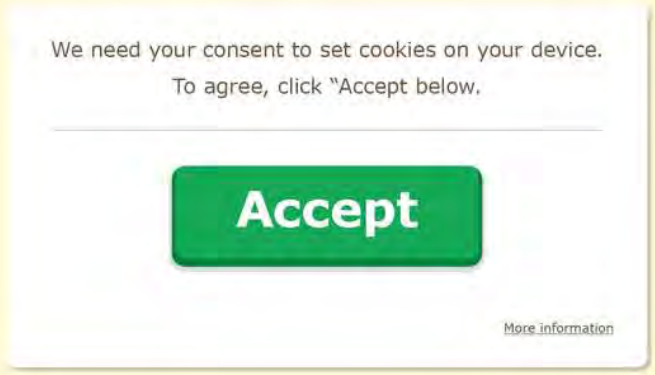
Non compliant

Example

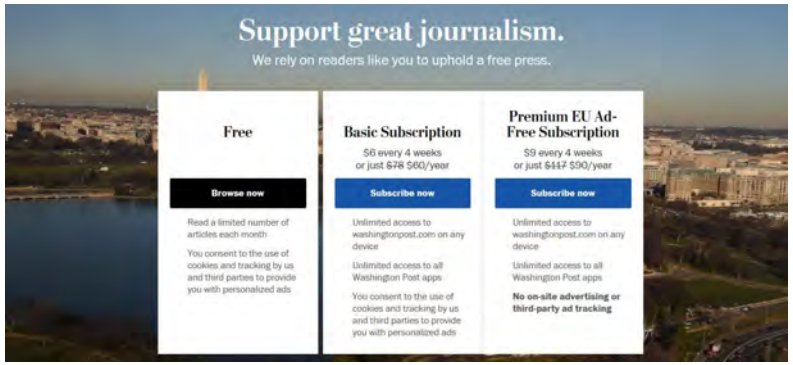
A consent mechanism that emphasises 'agree' or 'allow' over 'reject' or 'block' represents a non-compliant approach, as the online service is influencing users towards the 'accept' option.

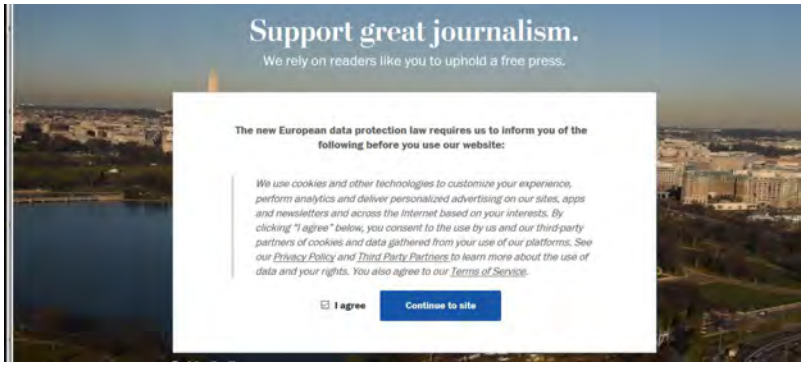


A consent mechanism that doesn't allow a user to make a choice would also be non-compliant, even where the controls are located in a 'more information' section.



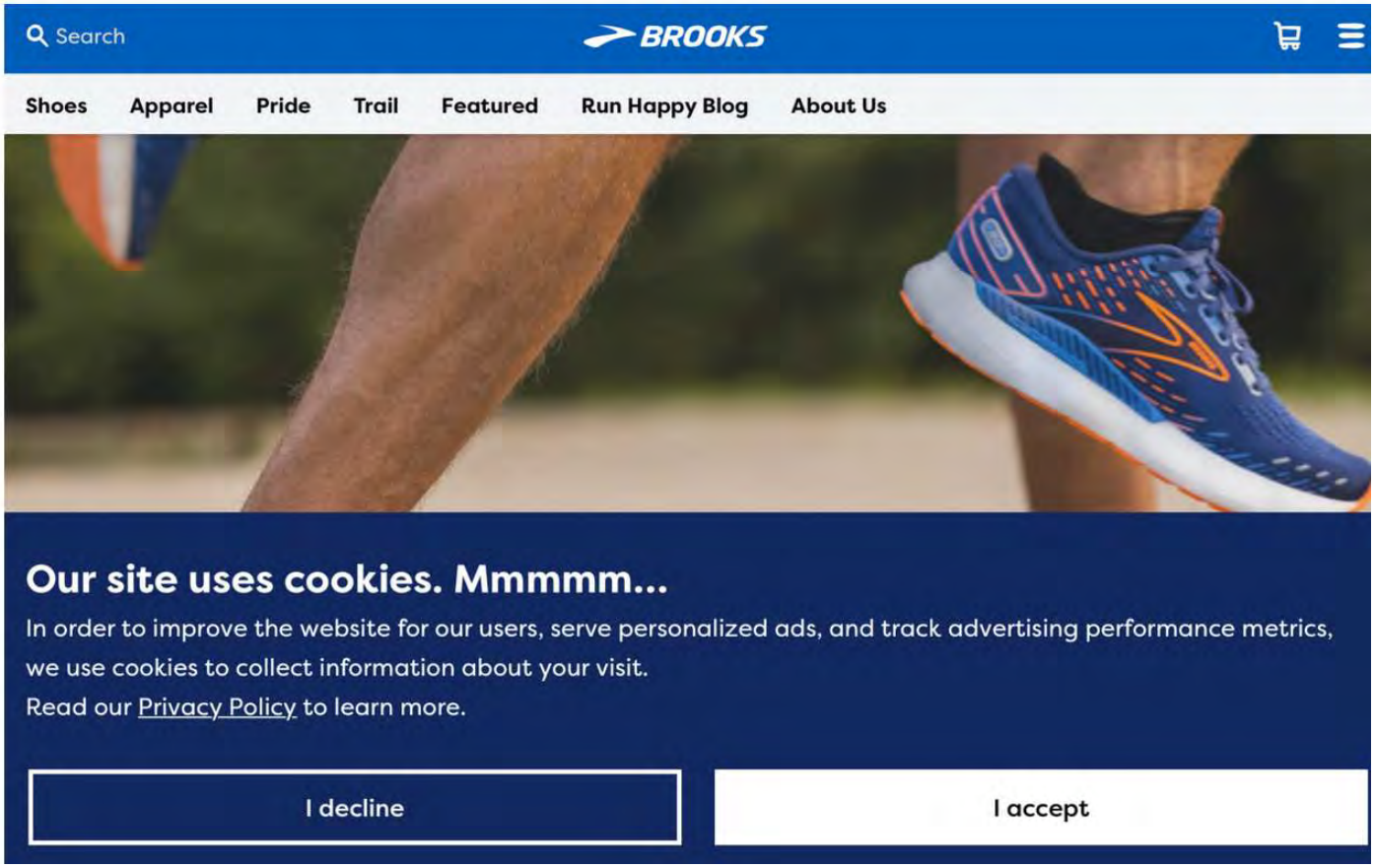
Compliant


Support great journalism.
We rely on readers like you to uphold a free press.
Free
Browse now
Read a limited number of articles each month
You consent to the use of cookies and tracking by us and third parties to provide you with personalized ads
Basic Subscription
$6 every 4 weeks
or just $78 $60/year
Subscribe now
Unlimited access to washingtonpost.com on any device
Unlimited access to all Washington Post apps
You consent to the use of cookies and tracking by us and third parties to provide you with personalized ads
Premium EU Ad-Free Subscription
$9 every 4 weeks
or just $117 $90/year
Subscribe now
Unlimited access to washingtonpost.com on any device
Unlimited access to all Washington Post apps
No on-site advertising or third-party ad tracking


Support great journalism.
We rely on readers like you to uphold a free press.
The new European data protection law requires us to inform you of the following before you use our website:
We use cookies and other technologies to customize your experience, perform analytics and deliver personalized advertising on our sites, apps and newsletters and across the Internet based on your interests. By clicking "I agree" below, you consent to the use by us and our third-party partners of cookies and data gathered from your use of our platforms. See our Privacy Policy and Third Party Partners to learn more about the use of data and your rights. You also agree to our Terms of Service.
I agree
Continue to site


Emojis para Twitter, haz tus Tweets aún más divertidos.
Facebook Social Plugins
Google Adsense
Google Analytics
Google+ Platform
Histats
Pinterest
Twitter Badge
Twitter Button
Emojis para Twitter
Twittear
Compartir 47
+1 47
available in the chrome web store
Esta web utiliza cookies. De las de comer no, de las otras
Vale!
No

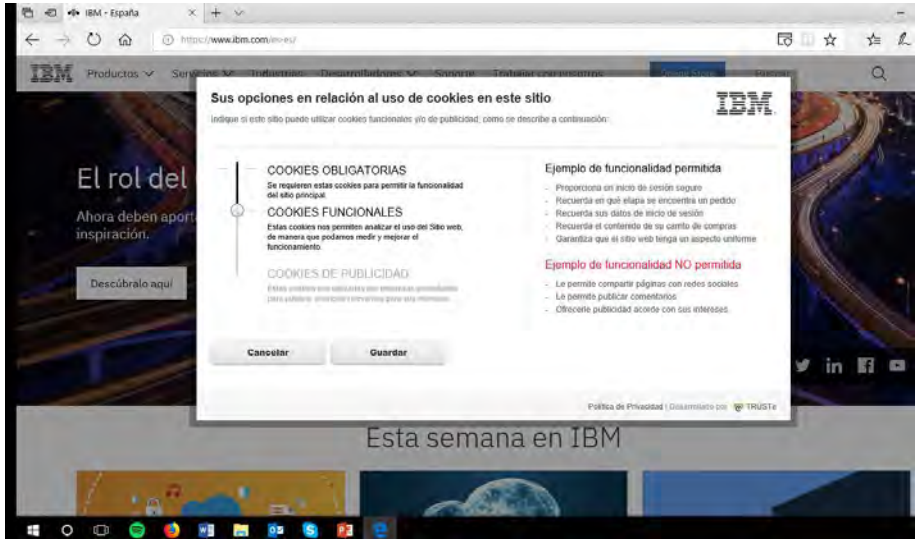

aerco-psm
INICIO
BLOG
FORMACIÓN
Curso de Branded Content #bro
Información
Programa
¡Aprovecha el 30% de descuento del curso!
El Branded Content se posiciona como uno de los protagonistas frente a la inversión publicitaria convencional y tradicional, cada vez más rechazada por el consumidor.
El Branded Content suaviza las diferencias entre lo que se supone que es simplemente publicidad y lo que es entretenimiento y es un recurso imponente a la hora de garantizar que el contenido de marca llegue a su target de la mejor forma posible.
Estudia las nuevas posibilidades que el Branded Content proporciona para analizar el cambio del rol del consumidor, y cómo deben relacionarse las marcas con él.
Aprende qué es un content curator y a saberlo diferenciar del community manager.
entra en aerco-psm
Usuario:
Contraseña:
Recordarme
ENTRAR
MÁS LEÍDOS
Aplicaciones para crear la foto de portada en Facebook
AERCO-PSM comparte su libro "Gestión de Comunidades Virtuales"
¿Cuánto debe ganar un Community Manager? Por Manuela Battaglini
Facebook Social Plugins
Twitter Button
aerco-psm
Este sitio web utiliza cookies para obtener datos estadísticos de la navegación de sus usuarios y ofrecerles una mejor experiencia de usuario. Para continuar navegando debes
ACEPTAR
su uso.


Search
BROOKS
Shoes
Apparel
Pride
Trail
Featured
Run Happy Blog
About Us
Our site uses cookies. Mmmmm...
In order to improve the website for our users, serve personalized ads, and track advertising performance metrics, we use cookies to collect information about your visit.
Read our Privacy Policy to learn more.
I decline
I accept

Compliant


Support the Guardian
Available for everyone, funded by readers
Contribute
Subscribe
Search jobs
Sign in
Search
International edition
The Guardian
For 200 years
It's your choice
When we make the Guardian available to you online, we use cookies and similar technologies to help us to do this. Some are necessary to help our website work properly and can't be switched off, and some are optional but support the Guardian and your experience in other ways.
For instance, we and our partners use information about you, your devices and your online interactions with us to provide, analyse and improve our services. This includes personalising content or advertising for you.
We use cookies and similar technologies for the following purposes:
Store and/or access information on a device
Personalised ads and content, ad and content measurement, audience insights and product development
You can find out more in our privacy policy and cookie policy, and manage the choices available to you at any time by going to 'Privacy settings' at the bottom of any page.
Are you happy to accept cookies?
To manage your cookie choices now, including how to opt out where our partners rely on legitimate interests to use your information, click on Manage my cookies.
Yes, I'm happy
Manage my cookies


IBM - España
Productos
Sus opciones en relación al uso de cookies en este sitio
Las cookies son importantes para el correcto funcionamiento de un sitio. Para mejorar su experiencia, utilizamos cookies para recordar detalles de inicio de sesión y proporcionar un inicio de sesión seguro, recopilar estadísticas para optimizar la funcionalidad del sitio y proporcionar contenidos a la medida de sus intereses. Haga clic en Aceptar y continuar para aceptar las cookies e ir directamente al sitio o haga clic en Establecer preferencias para ver descripciones detalladas de los tipos de cookies y elegir si desea aceptar determinadas cookies mientras permanece en el sitio.
Aceptar y continuar
Establecer preferencias
Política de Privacidad | Desarrollado por TRUSTe
El rol del
Descúbralo aquí
Siga a IBM
Esta semana en IBM


IBM - España
Productos
Sus opciones en relación al uso de cookies en este sitio
Indique si este sitio puede utilizar cookies funcionales y/o de publicidad, como se describe a continuación:
COOKIES OBLIGATORIAS
Se requieren estas cookies para permitir la funcionalidad del sitio principal.
COOKIES FUNCIONALES
Estas cookies nos permiten analizar el uso del Sitio web, de manera que podamos medir y mejorar el funcionamiento.
COOKIES DE PUBLICIDAD
Ejemplo de funcionalidad permitida
Proporciona un inicio de sesión seguro
Recuerda en qué etapa se encuentra un pedido
Recuerda sus datos de inicio de sesión
Recuerda el contenido de su carrito de compras
Garantiza que el sitio web tenga un aspecto uniforme
Ejemplo de funcionalidad NO permitida
Le permite compartir páginas con redes sociales
Le permite publicar comentarios
Ofrecerle publicidad acorde con sus intereses
Cancelar
Guardar
Política de Privacidad | Desarrollado por TRUSTe
El rol del
Descúbralo aquí
Esta semana en IBM

> Fines

France fines Apple for targeted App Store ads without consent
Meta to fight €390 million fine for breaching EU data privacy laws
Massive Twitter data leak investigated by EU privacy watchdog
LockBit ransomware goes 'Green,' uses new Conti-based encryptor
Monero hard fork makes hackers' favorite coin even more private

Thanks for your attetion :)

Any doubt?

paulaortiz@gmail.com