

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

**Introduction to the GDPR
Maciej Gawronski**

Athens, 14 October 2022



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



**PERSONAL DATA
PROTECTION OFFICE**

Warsaw, 14 September 2021

To whom it may concern,

I confirm that Mr Maciej Gawronski is a prominent legal advisor and an expert involved in the development of personal data protection. Moreover, he is a very good practitioner with broad knowledge, who has been actively supporting personal data protection in Poland for many years. By active participation in numerous international conferences and other events related to personal data protection, he contributes to the discussion on the main and the most important directions in this area. As regards popularizing social awareness of personal data protection, his active participation in social media with a valuable voice on issues related to personal data protection should also be appreciated.

He possesses deep understanding of information technology, cloud computing and cybersecurity and his vast knowledge is recognized by national and international legal rankings, naming him among the leading legal experts in these fields.

He cooperated as an expert of the European Commission on cloud computing agreements and a consultant of the Article 29 Working Party, now replaced by the European Data Protection Board (EDPB). During the period accompanying the work on the implementation of the reform of the personal data protection regime in the EU, he made a significant contribution to the development of tools to support the implementation and application of the provisions of the General Data Protection Regulation.

He is the author of many scientific and practical studies on personal data protection, which he regularly publishes both in Poland and abroad. He has published extensively, being the editor and co-author of bestselling, innovative books on the General Data Protection

Regulation and dozens of articles which relate both to law and technology. In his papers he creates good data protection standards.

He is an experienced lecturer, appreciated by students and listeners in particular for his practical and substantive presentation of data protection issues. As a legal advisor specializing in the right to personal data protection and privacy, he contributes to raising the level of knowledge by advising on how to act in accordance with the law in the era of rapid development of modern technologies and digital transformation.

Mr Maciej Gawroński is a person who values dialogue in his professional work thus being open to sharing knowledge. He contributes to solving problems, finding reasonable, practical and unexpected solutions and refraining from useless criticism in the field of personal data protection, explaining complicated things in an easily, understandable manner.

Yours faithfully,

Jan Nowak

The President of the Personal Data Protection Office



Maciej Gawroński • Piotr Biernatowski

**Jak pisać
pisma procesowe
i prowadzić komunikację
w sporze**

czyli książeczka o pisaniu pism



 Wolters Kluwer

1. **GDPR - general characteristics**, basic concepts
2. **Sprint through the rules** for controllers:
 - (1) basic legality
 - (2) rights of individuals (DSRs)
 - (3) security
 - (4) entrustment of data, joint controlling, data sharing
 - (5) data export / data transfers
 - (6) liability - remedies
3. **GDPR and compliance** in an organization - responsibilities and division of roles in an organization DPO v DPCO

Technology vs regulation



<https://www.youtube.com/watch?v=5oPsvq81n2A>

GDPR - General Characteristics

GDPR – TOWARDS UNIFORM RULES



GDPR - what's new?

- Risk-based approach?
- Accountability – presumption of guilt
- Data retention
- Data Subject Rights - many
- Privacy by design, Privacy by default
- Register of Data Processing Activities
- Breach notification
- Data Protection Impact Assessment (DPIA)
- Data Protection Officer (DPO)
- Direct liability of processors (I am sorry, my fault)
- Fines and liability
- TFD data export

What does GDPR consist of?

The GDPR is divided into the following chapters:

- 0. Recitals (173 recitals take up about 35% of the GDPR text)**
- I.** General provisions - including territorial and material scope
- II.** Principles
- III.** Rights of the data subject
- IV.** Controller and processor
- V.** Transfer of personal data to third countries or international organisations
- VI.** Independent supervisory authorities
- VII.** Cooperation and consistency
- VIII.** Remedies, liability and penalties
- + **Exceptions** Provisions for specific processing situations
- + Delegated and implementing acts



PILLARS

Legality – obligations to implement

Rights – data subject requests to respond

Security - processes to design and maintain

FOUNDATIONS

Risk - risk (for data subjects) a measure of required diligence

Accountability - duty to explain (presumption of guilt)

OTHER

Data processing supply chain management

Transfers - outside the EU

Table of Contents	Functional Breakdown
Recitals	Interpretation
CHAPTER 1. General provisions	Compliance I
CHAPTER 2. Principles	
CHAPTER 3. Rights of data subject 12, 13, 14	
CHAPTER 3. Rights of data subject 12, 15-22	Complaints management
CHAPTER 4. Controller and processor 24, 25.1, 26-30, 35, 36, 37-39	Compliance II
CHAPTER 4. Controller and processor 32, 25.2	Security
CHAPTER 4. Controller and processor 33, 34	Consequences – Breach management
CHAPTER 5. Transfers of personal data to third countries or international organizations	Compliance III – Data exports TFD
CHAPTER 6. Independent supervisory authorities	For Authorities
CHAPTER 7. Cooperation and consistency	
CHAPTER 8. Remedies, liability and penalties	Consequences – Legal proceedings
CHAPTER 9. Provisions relating to specific processing situations	Exceptions (e.g. journalists)
CHAPTER 10. Delegated acts and implementing acts	For Authorities
CHAPTER 11. Final provisions	

GDPR - THREE PILLARS AND TWO FOUNDATIONS

LEGALITY

RIGHTS

SECURITY

ACCOUNTABILITY

RISK ...ASSESSMENT

OBLIGATIONS

Article 5

Article 6

Article 7

Article 8

Article 9

Article 10

Article 11

Article 12

Article 13

Article 14

Article 15

Article 16

Article 17

Article 18

Article 19

Article 20

Article 21

Article 22

Article 24

Article 25

Article 26

Article 27

Article 28

Article 29

Article 30

Article 32

Article 33

Article 34

Article 35

Article 36

Article 37

Articles 46

Articles 49

Proactive obligations

- 1) **Inventory** of data processing operations,
- 2) **Design and documentation** (i.a. data processing policy, records of processing activities, specific procedures, LIA, DPIA, consents, information obligation, data processing agreements, SCCs, transfer impact assessment),
- 3) **Security** (security policy, data processing risk analysis,, TOMs).

Data Subjects Rights

- to be informed (exhaustive, concise, readable, accurate)
- to access data and to a copy of data
- to rectify data
- to erasure
- to restrict processing
- to data portability
- to object due to particular situation
- to a human intervention in automated processing

Reactive obligations

Breach Management

- breach **notification** (supervisory authority)
- breach **communication** (data subjects),
- a need for speed 72h

Legal Proceedings



G+P MAIN CHARACTERISTICS



Ambiguity

GDPR is built on a set of principles



- 1) lawfulness, fairness and transparency (5.1.a GDPR)
- 2) purpose limitation (5.1.b GDPR)
- 3) data minimisation (5.1.c GDPR)
- 4) accuracy (5.1.d GDPR)
- 5) storage limitation (5.1.e GDPR)
- 6) integrity and confidentiality (5.1.f GDPR)
- 7) Accountability (5.2 GDPR)

- art. 32 GDPR – security obligation

*...the controller and the processor shall implement **appropriate** technical and organisational **measures** to ensure a level of security appropriate to the risk*

24.1, 25.1

The guidelines are not by accident vague

"It's a question of which side of the table you're sitting on. As a regulator, we have tasks too. You don't have to fulfill my tasks, so don't expect me to fulfill yours."

Andrea Jelinek

Chair of the European Data Protection Board

approx. 60 separate sets of guidelines

https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en?f%5B0%5D=opinions_publication_type%3A64

<https://iapp.org/news/a/new-wp29-chair-talks-enforcement-role-of-the-dpo/> accessed 26.04.2018





Risk-based approach // Risk assessment

GDPR 24.1.

Taking into account the nature, scope, context and purposes of processing as well as the **risks of varying likelihood and severity** for the rights and freedoms of natural persons, the controller shall implement **appropriate** technical and organisational **measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

GDPR 32.1.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the **risk of varying likelihood and severity** for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a **level of security appropriate to the risk**

DIRECTNESS

The GDPR applies to everyone across the Union, in **fact every entity except ordinary consumers ...at home, ie:**

- **individuals running businesses,**
- **legal persons:** joint-stock company, limited liability company, cooperative, foundation, registered association, state enterprise, religious association, research institute, political party, trade union, ecclesiastical legal person,
- **public authorities**
- **other entities**, e.g. partnership, limited partnership, association, university...
- **neighbours...**
- **bloggers, influencers...**

Full implementation of GDPR means hundreds of obligations imposed on Controllers.

MEASURABILITY

- 1** month to respond to a data subject's request
- 3** months (max) to comply with the person's request
- 72** hours to notify the SA of a security breach

SEVERITY

Astronomical fines "effective, proportionate and dissuasive"
(GDPR 83.1.).

- up to € 20/10 M
- up to € 4/2% of the worldwide turnover when it's > €500M

Penalty matrix - 18+ criteria (83.2. GDPR)

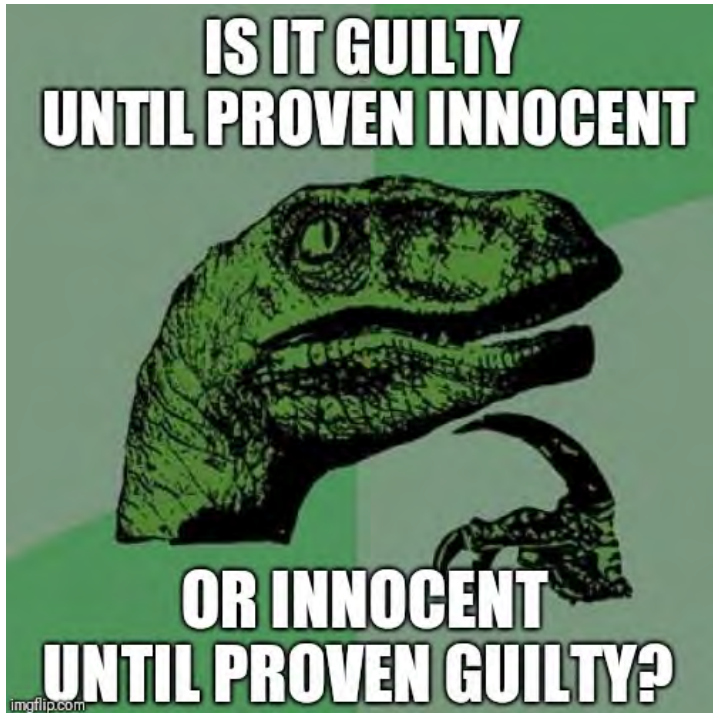
"Confiscation" of benefits and savings:

Article 83.2.k GDPR: any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefit derived directly or indirectly from the breach or loss avoided.

b) Course of overall **number** of fines (cumulative):



PRESUMPTION OF GUILT a.k.a. ACCOUNTABILITY



GDPR 5.2.

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

GDPR 24.1.

...the controller shall implement appropriate technical and organisational measures to ensure and to be able **to demonstrate** that processing is performed in accordance with this Regulation

GDPR 82.3.

The controller or processor shall be exempted from liability pursuant to paragraph 2 if the controller or processor proves that they are in **no way at fault** for the event giving rise to the damage.

Right to compensation and liability

82.1. Any person who has suffered material or non-material damage [...] shall have the **right to receive compensation from the controller or processor** for the damage suffered

82.2. Any controller involved shall be liable [...]. A processor shall be liable [...] 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

82.4. A controller or processor shall be exempt from liability [...] if it **proves that it is not in any way responsible** for the event giving rise to the damage

PRINCIPLE OF PROPORTIONALITY



Where are we?

GDPR:

- no full unification of data protection rules
- BUT a step towards

GDPR 2?

2 big 2 B liable?



Sprint through obligations of controllers

GDPR – Basic concepts

Controllers use data for themselves

Every organization is a data controller

*"**controller**" means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*



Processor

Processor has data on behalf of somebody else, usually for money.

"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller



a) recipient:

- controller
- processor
- natural person

b) „not recipient” – authority conducting particular legal proceedings (*particular enquiry*)

*‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. **However, public authorities** which may receive personal data in the framework of a **particular inquiry in accordance with** Union or Member State **law** shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;*

bad legislation

personal data – every information we can attribute to a person, including so-called content and metadata (IP)

(content, membership file, employee file, paper list of employees, decisions on granting allowances, data of employees and their families for the purpose of granting allowances, data of employees for the purpose of holding a pre-trade union referendum, data obtained within the framework of trade union consultations).

- Personal data can be "ordinary" (regular) or "special categories" (sensitive) and also criminal.

"**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;

"**special categories of data**" are listed in Article 9.1 of the GDPR.

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

Examples of data categories

- **Basic identification data**
- Identification data allocated by public authorities
- Electronic identification data
- Electronic location data
- Biometric identification data
- Financial identifying information
- **Information on financial resources**
- Commitments and expenses
- Solvency
- Loans, mortgages, lines of credit
- **Financial assistance**
- Insurance policy details
- Pension plan details
- Financial transactions
- Compensation
- Official acts
- Agreements and settlements
- Permits
- Personal details
- Military service status
- Immigrant status
- Description of appearance
- Private habits
- Addictions
- Lifestyle
- Travel and movement data
- Contacts with others
- Holdings
- Social functions
- Complaints, incidents and accidents
- Awards
- Use of media
- Psychological data
- Marriage or other form of relationship
- Marriage history
- Details of other family members or household members
- Hobbies and interests
- Membership (other than service, political, trade union)
- Legal information on suspicions
- Information regarding convictions and sentences.
- Information on judicial action
- Data on administrative penalties
- Consumption habits
- **Residence data**
- Physical health data
- Mental health data
- Data on risky situations and behaviour
- Genetic data relating to population studies, gene testing, etc.
- Recovery data
- Education and training
- Academic teaching
- Publications
- **Occupation and employment**
- Current employment
- Recruitment
- Completion of work
- Career
- Absences and adherence to work order
- Occupational medicine
- **Remuneration**
- Assets held by the employee
- Organisation of work
- Evaluation
- Training for the position
- Credentials,
- Levels of competence
- Use of technology
- Data on racial or ethnic origin
- Data on sex life
- Political views
- Political connections
- Membership of advocacy groups, paramilitary organisations
- **Trade union membership**
- Religious or philosophical beliefs
- Beliefs
- Video recordings
- Image
- Sound recordings

Processing of personal data

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

Can data controller process data unconsciously?
Unwillingly?



effective loss of control over data

*„Personal data breach" means a [1] **breach of security** [2] **leading to** [consequences] the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;*

When does GDPR apply?

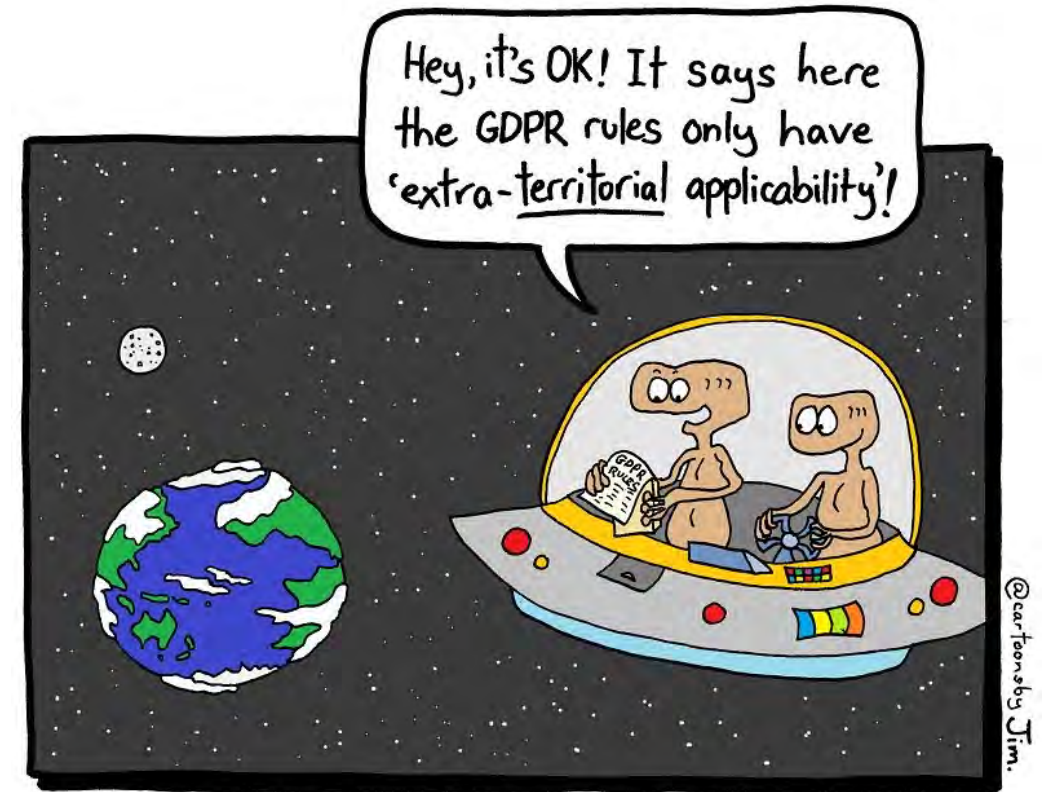
2.1 GDPR

This Regulation applies to (1) the processing (2) of personal data by (3) wholly or partly automated means and (4) to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

G+P Where does GDPR apply? EVERYWHERE

- If your organisation is based in EU
- Wherever you are If your organisation:
 - 1) addresses your offer to EU residents
 - 2) monitors people behaviour in EU

No, ETs should not be so happy. GDPR DOES have an extra-terrestrial effect.



<https://twitter.com/cartoonsbyjim/status/1002450296834912256>

GDPR Details

Legality 1

Lawfulness of data processing

Legality 1 - Principles

- data processing principles - 5
- basis for processing - 6
- consent requirements - 7
- minors' protection in Internet - 8
- special categories data (ex sensitive) - 9
- criminal data - 10
- „unidentified” data - 11
- information obligation - 13, 14
- tracking recipients 19.1st

Legality 2 - Controller and processor

- risk-based approach and accountability principles - 24
- privacy by design - 25.1
- joint controlling - 26
- EU representative
- data processor - 28
- documented instructions - 29
- register of activities and register of categories - 30
- DPO - 37-39

Legality 3 - Transfers of data outside the EU only under additional conditions - 44

- Standard Contractual Clauses + TIA
- Adequacy decision
- Treaty
- Contract performance
- Explicit consent informed of possible risks
- Absolute necessity

We should process personal data in accordance with the following principles:

- a) Lawfully, fairly and transparently (lawfulness/legality)
- b) For specific purposes only (purpose limitation)
- c) Only necessary data (data minimization)
- d) Ensure data are correct and up to date (accuracy)
- e) No longer than necessary (temporality / storage limitation)
- f) Securely (integrity and confidentiality)

very vague and general BUT

The controller [...] must be able to **demonstrate compliance ("accountability")**.

Ordinary/regular data

- a) consent
- b) performance or conclusion of the contract
- c) controller's legal obligation (e.g. AML)
- d) someone's vital interests
- e) public task, public authority
- f) legitimate interest of controller / third party (witnesses, opponents, etc.)

Special categories also

- a) express consent
- b) employment and social law
- c) vital interests + unconsciousness/underage/ incapacitation
- d) NGOs...
- e) publically disclosed data (Elton John not Hunter Biden. HB is a journalist exception)
- f) claims enforcement/defense
- g) letter of law
- h) health care (occupational medicine, diagnosis, health care ...)
- i) public health (abused for sanitarism)
- j) archives, statistics, scientific and historical research

Information obligations



GDPR 13 and 14

- Identity, contact details of controller, DPO, representative
- Purposes of processing, legal basis
- Legitimate interests (e.g. marketing) if invoked
- Information about recipients of personal data or categories of recipients, if any (other companies if we want to e.g. sell the data, subcontractors - processors, but not state authorities)
- Where applicable, information on transfers to a third country
- Categories of data obtained, if not from the person concerned
- Information on rights
- Information on obligations (if data must be provided)
- Information about automated decision-making (including related profiling)
- Information about the source of the data, if not from the person concerned

G+P In what situations and when do we inform you about data processing?

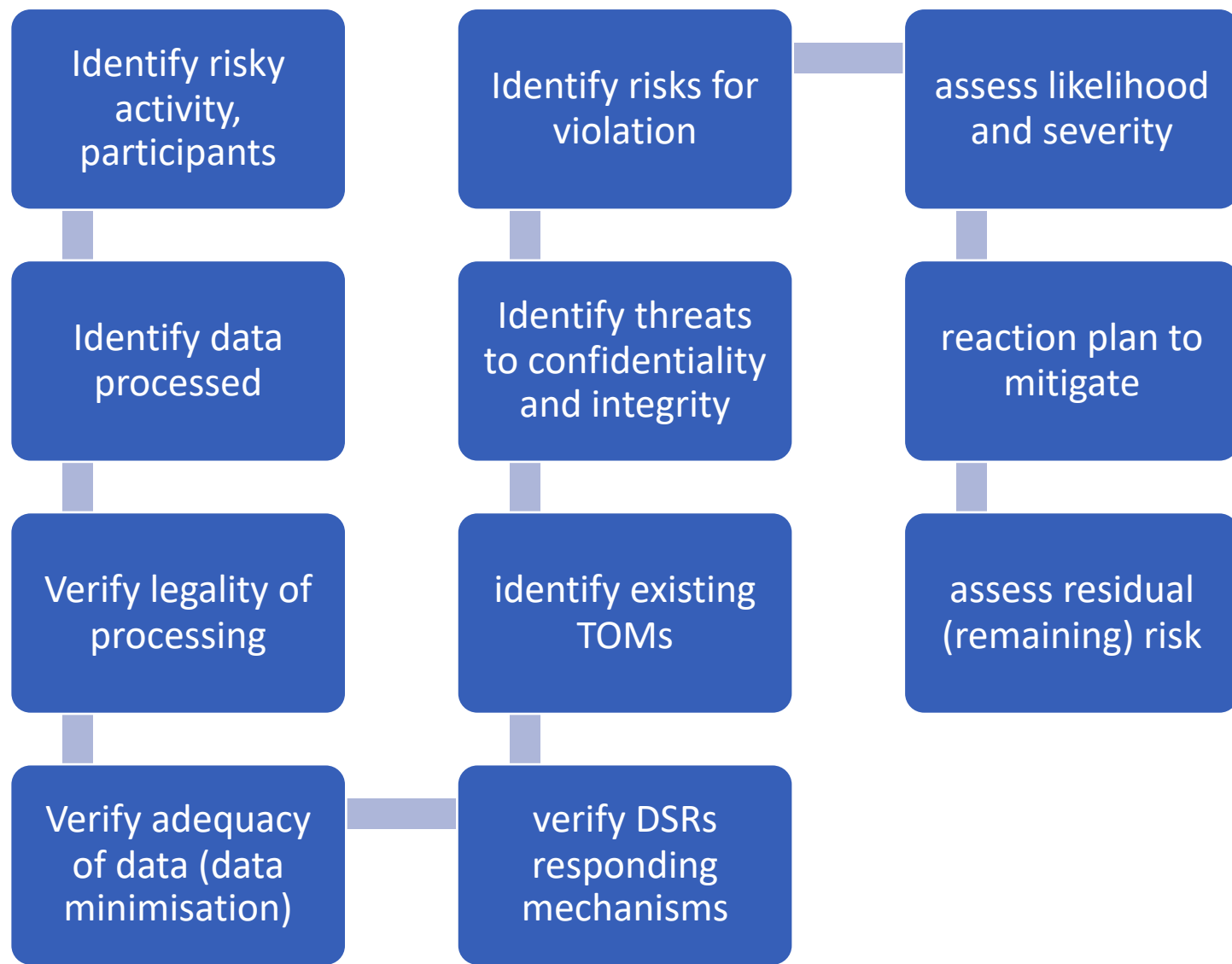
- When we collect [data directly from data subjects](#) (GDPR 13) - we inform when we obtain data from a person
- When [we obtain data by other means](#), e.g. from publicly available sources such as LinkedIn (GDPR 14) - we inform within one month. We inform as soon as possible, within a month or at the first contact or at the disclosure of the recipient's data, whichever is sooner.
- When [we change the purpose of data processing](#) (GDPR 13(3) and 14(4))
- When [we execute a data access request](#) (GDPR 15) - within one month of the request (as a general rule, extendable by 2 months).

Privacy by design – designing privacy

GDPR 25.1

Taking into account the [1] state of the art, the [2] cost of implementation and the [3] nature, scope, context and purposes of processing as well as the [4] **risks of varying likelihood and severity** for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement **appropriate technical and organisational measures**, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

DPIA - CNIL



I. Data processing agreement - Article 28 GDPR

II. Joint control - Article 26 GDPR



DATA SUBJECT'S RIGHTS

- Metrics - 12
- information obligation direct collection - 13
- information obligation indirect collection - 14
- data access, data copy - 15
- rectification - 16
- removal - 17
- data limitation - 18
- notification to and about recipients - 19
- **data portability - 20**
- objection - 21
- automatic processing - 22

Rights of data subjects

Reactive obligations

- to access data and to a copy of data
- to rectify data
- to erasure
- to restrict processing
- to data portability
- to object to processing due to particular situation
- to object to processing for marketing purposes
- to a human intervention in automated processing

and many more...

- **Right to be informed about data collection**
- **Right to access to and copy of data (15)**
- **Right to rectify (16)**
- **The right to erasure /be forgotten (17)**
- **Right to restrict processing (18)**
- **Right to know about recipients (19.2nd)**
- **Right to data portability (20)**
- **Right to exceptional and marketing objection (21)**
- Right to withdraw consent
- **Right of appeal against automatic decision (22)**
- Right to response (prohibition of ignoring)
- The right to "readability"
- Right to facilitate (to guide)
- Right to deadlines
- Right to information about rights
- Right to equally easy consent withdrawal
- Right to information on data recipients
- Option for convenient electronic handling
- **Right to know about a data breach**
- **Right to complain and appeal**
- **Right to court damages**
- **Right to an NGO support**

GDPR 15.1

Right to:

confirmation as to whether data are being processed

access to the data

and to information on: **[a]** purposes, **[b]** categories, **[c]** recipients, **[d]** retention, **[e, f]** rights, **[g]** source, **[h]** automated decision-making, profiling, its rules and consequences - corresponds to the right to information

Right to a copy of the data

GDPR 15.3 The controller shall provide the person with a copy of the data relating to them.

For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.

If the data subject requests a copy by electronic means and unless he or she indicates otherwise, the information shall be provided by commonly used electronic means.

GDPR 15.4 The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

- **Notice & Takedown – i.e. the procedure for objection by others + denial of release due to own rights and secrets**

GDPR 16

- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
- Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

GDPR 17

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- withdrawal of consent
- **object** to the processing **and there are no overriding legitimate grounds for processing** (with direct marketing there will be none - GDPR 21.2)
- the data have been unlawfully processed
- personal data must be deleted in order to comply with a legal obligation
- **the personal data was collected in connection with the offering of information society services** (as in direct marketing)

Limitation of processing

- a) Data subject questions accuracy of data
- b) processing is unlawful and data subject objects to erasure of the data, requesting instead that the use of the data be restricted;
- c) the controller does not need the data, but the person needs them to establish, assert or defend a claim;
- d) for the duration of the specific objection (whether the controller's grounds override the grounds for objection).
- practical solutions:
 - 1) no one will come forward with this on their own because they won't understand
 - 2) we will propose a restriction in lieu of other rights - e.g., for the purpose of storing surveillance data, if we are afraid to disclose the recording directly to the data subject

Obligation to track and notify the recipients

GDPR 19

- The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out 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.

Right to data portability

GDPR 20

- The data subject shall have the right to **receive** the personal data concerning him or her, which he or she **has provided to a controller** and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
 - the processing is based on consent or contract,
 - the processing is automated
- In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
- Exceptions: public interest or exercise of official authority entrusted to the controller.
- The right to data portability must not adversely affect the rights and freedoms of others (the issue of data rights and the lawfulness of data - analogy to the grounds for notice & takedown)

Right to object: special situation and direct marketing

GDPR 21

- The data subject shall have the **right to object**, on grounds relating to his or her **particular situation**, at any time to processing of personal data concerning him or her including profiling based on those provisions.
- The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- Where personal data are processed for the purposes of **direct marketing**, the data subject shall have the **right to object** at any time to processing of personal data concerning him or her for such marketing, including profiling, to the extent that the processing is related to such direct marketing. If the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes
- At the latest on the occasion of the first communication with the data subject, the data subject shall be expressly informed of the right to object.

GDPR 22

The right not to be subject to a decision producing **legal or similarly significant effects** which is based **solely on automated processing**, including profiling, unless

- is necessary for the conclusion or performance of a contract with a person
- lawful
- is based on an explicit consent

In cases (1) and (3), the Controller shall implement appropriate safeguards, at least the rights to **obtain human intervention** by the controller, to express one's point of view and to challenge that decision.

Security

- *Privacy by default 24.2 (Security)*
- Security and risk analysis - 32 (Security)
- Data Protection Impact Assessment – 35 (Compliance)
- Prior Consultation - 36 (Sepuku)
- Breach notification - 33 (Consequences)
- Breach communication - 34 (Consequences)

Taking into account the (1) state of the art, (2) the costs of implementation and (3) the nature, (4) scope, (5) context and (6) purposes of processing as well as **(7) the risk of (8) varying likelihood and (9) severity** for the rights and freedoms of natural persons, the controller and the processor shall implement **appropriate** technical and organisational measures to ensure a level of security **appropriate** to the risk, including inter alia as appropriate:

- pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services [CYBER SECURITY//BUSINESS CONTINUITY].
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident - DISASTER RECOVERY
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing - TESTING

G+P Data Security Risk Assessment

- GDPR 32.2 risk assessment

In **assessing the appropriate level** of security account shall be taken in particular of the **risks** that are presented by processing, in particular from accidental or unlawful **[1]** destruction, **[2]** loss, **[3]** alteration, **[4]** unauthorised disclosure of, or **[5]** access to personal data transmitted, stored or otherwise processed.

- GDPR 24.1 and 25.1 and 32.1



Privacy by default – Minimisation!

GDPR 25.2

2The controller shall implement appropriate technical and organisational measures for ensuring that, **by default, only personal data which are necessary** for each specific purpose of the processing are processed. That obligation applies to the **[1]** amount of personal data collected, the **[2]** extent of their processing, the **[2]** period of their storage and **[3]** their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons

How about this?



© D.Fletcher for CloudTweaks.com

Data transfer to a third country

Principle

- Free movement of data within the European Economic Area
- No specific regulation for intra-EEA transfers
- Data transfer = data processing
- Transfers of data outside the EEA- transfer of data to third countries + international organisations.

Transfers of data outside the EEA - a two-step approach

- General obligations + additional obligations provided for in Chapter V of the GDPR

What is data transfer outside the EU?

Transfer of data to third countries = transfer of data outside the European Economic Area

No legal definition of transfers to third countries in the GDPR

Under the proposed definition:

any transfer of personal data that is actively made available to a limited number of parties or identified parties with the knowledge of the transferor or with the intention of providing the recipient with access to the personal data

a transfer of personal data which leads to the personal data 'crossing' a 'secure' border into the European Economic Area (EEA)

Basis for transfers to third countries

Article 45 GDPR

Pursuant to a decision of the European Commission

The Commission may decide that certain countries provide adequate protection for personal data:

EC Decisions:

- | | |
|--------------------------------|---|
| 1. Switzerland (2000/518/EC) | 10. Uruguay (2012/484/EU) |
| 2. Canada (2002/2/EC) | 11. New Zealand (2013/65/EU) |
| 3. Argentina (2003/490/EC) | 12. USA – Privacy Shield (2016/1250) (self-certification). |
| 4. Guernsey (2003/821/EC) | 13. Japan - C(2019) 304 |
| 5. Isle of Man (2004/411/EC) | 14. Republic of Korea – C(2021) 9316 |
| 6. Jersey (2008/393/EC) | 15. UK – new adequacy decision |
| 7. Faroe Islands (2010/146/EU) | |
| 8. Andorra (2010/625/EU) | |
| 9. Israel (2011/61/EU) | |

Basis for transfers to third countries

Article 46 GDPR

"subject to appropriate safeguards", which means:

Based on the following specific legal instruments:

- a) a legal instrument between public authorities and bodies (e.g. an administrative agreement between a Member State authority and a non-EU country authority)
- b) Binding Corporate Rules (47 GDPR) - internal agreements within a corporate group (group of companies)
- c) **standard data protection clauses** - model contract terms (adopted by the EC, adopted by the national supervisory authority)
- d) approved code of conduct
- e) approved certification mechanism
- f) contract or administrative arrangement approved by the supervisory authority

Additional grounds for transfers to third countries

Article 49 GDPR

Specific grounds for data transfer:

- a) **risk-based consent**
- b) **performance of a contract** or for the **conclusion of a contract at the** request of a person
- c) concluding or performing a contract, where it is in the interest of the data subject, who is not party to the contract
- d) **public interest**
- e) **redress**
- f) **to protect someone's vital interests** where the data subject is incapable of giving consent: (i) physically, (ii) legally
- g) transfer from the public register under normal access conditions

Transmission really specific Article 49(2) GDPR

The transfer of data may take place on the basis of specific grounds which are: the **compelling legitimate interests of the controller**:

To benefit from the export of data under Article 49(2) requires that:

- a) the transfer was not repetitive
- b) concerned a limited number of people
- c) was necessary for the legitimate interests of the controller (en. *compelling*, i.e. "compelling", fr. *imperieux*, i.e. "vital" interests of the controller)
- d) the interests, rights and freedoms of the data subject are not overridden,
- e) the Controller made a comprehensive assessment of the situation and consequently
- f) ensure adequate safeguards for the protection of personal data,
- g) informed the supervisory authority,**
- h) informed the data subject.

G+P Transfers of data to third countries outside the EEA

What should I do?

- identify situations **where we transfer data outside the EEA**,
- **verify contacts with counterparties outside the EEA**, transfer of data to the parent company,
- **review the manner of communication** (monitoring of shadow IT) and use of public cloud services by our organization as well as processors (subcontractors).

- The most practical basis for transferring data outside the Union is the **standard data protection clauses**
- Consent is an inconvenient basis for data export because it can be revoked at any time
- The duty of information of data subjects to whom we transfer data outside the EEA exists and when transferring on the basis of:
 - standard data protection clauses
 - decisions on data protection adequacy

G+P Judgment Schrems II

Maximilian Schrems, initiator of the ruling overturning the Safe Harbour (2015) and Privacy Shield (2020) program decisions

Judgment of the CJEU C-311/18 of 16.07.2020 so called Schrems II¹

- **CJEU invalidates Privacy Shield** (lack of procedural safeguards for non-US persons subjected to mass electronic surveillance)
- **CJEU leaves in place SCC** but it is not necessarily legal to transfer data on the basis of SCC² - no more mechanical signing of SCC , **because of risk of eavesdropping by NSA**
- **SCCs to U.S. are now "suspect"**

and then what happened?

¹link: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=9890094>).

² For more on the verdict : <https://gppartners.pl/pl/co-z-uslugami-chmurowymi-po-wczorajszym-wyroku-tsue-uniewazniajacym-transfery-do-usa/>



EDPB guidelines or 4 steps to where?

1. **map data transfers**
2. **Establish a legal transfer tool** (SCC, ad hoc clauses, BCRs, consent, Article 49 GDPR exception).
3. **evaluate the law of the** target country - does it undermine the effectiveness of the transfer tool?
4. **apply additional** protective **measures** (examples in the Annex to the Guidelines)
5. document
6. repeat regularly

"if you still wish to proceed with the transfer, you should look into other relevant and objective factors, and not rely on subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with EU standards."

FACEPALM - and why so? because they figured out that the CJEU logic doesn't pass the probability test according to the disclosure statistics published by the giants?

G+P EDPB - Recommendations for Basic Guarantees

Evaluate whether the law of the destination country undermines the effectiveness of the transfer tool

- a) Are the data access rules clear
- b) Is the necessity and appropriateness for legitimate access purposes ensured
- c) Is there an independent access control mechanism
- d) Do people have effective legal tools

Poland would not pass this test.



Consequences of Schrems II - What to do?

Assess the risks to rights and freedoms, including in particular:

- try not transfer content to the US 😂
- Evaluate the potential for interest in our clients or others whose data we send to the U.S. by U.S. services (**NOTE:** EDPB doesn't like that approach);
- assess whether the NSA's eavesdropping on our telemetry or so-called user data poses a real risk to those individuals (it **doesn't**, unless we know we're working with intelligence, counterintelligence, international crime, or states, in which case maybe it does 😏)
- delegate to a client - inform them of the risks? "If you're a terrorist or you're contracting assassinations in addition to drug trafficking, we advise against using our services because we transfer data to the U.S."
- to see if/how our CP "handled" Schrems II.

Data export disaster

~~Safe Harbor~~ -> Schrems I

Schrems* I -> Privacy Shield

~~Privacy Shield~~ -> Schrems II

Schrems II -> Privacy Shield 2.0 ?

*We're not asking where Mr Schrems gets his funding from

BRIEFING ROOM

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

OCTOBER 07, 2022 • PRESIDENTIAL ACTIONS

<https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>

WHO WOULD WIN?

A POWERFUL UNION OF
EUROPEAN COUNTRIES,
A WESTERN SUPERPOWER
AND SOCIAL MEDIA



ONE AUSTRIAN BOI



GDPR and compliance

Responsibility

Division of roles in the organization

Liability for non-compliance with GDPR

A. PERSONAL

- General **criminal**
- **Criminal** obstruction
- **Employee**
- **Disciplinary**

B. Controller RESPONSIBILITY

- **Reputational**
- **Business** (contractors)
- **Financial**
- **Civil**: GDPR, tort, contractual
- **Administrative**

Who can be sanctioned? Controller, Joint Controller, Processor, Sub-Processor, Certifier (42, 43 GDPR), Code Monitor (Article 41(4) GDPR) = **Organization = Board of Directors**

What is he responsible for?

- special care, utmost care, risk principle

How do you protect yourself? - on the following slides

Who will hold us accountable?

- Individual customers
- Former employees
- Competition
- GDPR Law Offices and District Courts
- Large institutional customers
- Important processors (service providers such as call centres)
- Niebezpiecznik.pl, ZaufanaTrzeciaStrona
- Newspapers
- Prosecution
- The President of the Data Protection Authority

When is the threat of penalties real?

If we implement GDPR well, are we safe? **NOT EXACTLY**

- when we're on the front page of the newspaper
- when our personal data leaks (do we fall victim to a hacking attack?)
- ...when someone reports us. Who? Customers, employees, unions. Why? Why not?
- when we process data without a legal basis (e.g. after withdrawal of consent)
- when we fail to handle individual rights (higher penalty)
- when the assistant sends "send to all" instead of "bcc"
- when we unlawfully use a non-EU cloud... (higher penalty).

Greater Punishment

Violation of processing principles:

- 1) **Article 5 principles**
- 2) **legal grounds for processing under article 6 and 9 GDPR**
- 3) conditions for consent in Article 7 of the GDPR
- 4) **the rights of the** data subjects, as referred to in Articles 12-22 of the GDPR (so also the SLA: transparent information, timing, facilitation...)
- 5) data transfer (export) (Articles 44-49 GDPR)
- 6) infringement of Member State law obligations under Chapter IX of the GDPR - national data protection rules in employment law - Article 88 GDPR),
- 7) inobedience of regulators (Article 58(2) GDPR, Article 58(1) GDPR)

Smaller Punishment

A lesser fine for violation of other obligations, including

- 1) **security**
- 2) records
- 3) DPO
- 4) Children's data processing
- 5) unidentified data
- 6) **privacy by design, privacy by default**
- 7) minor breaches not amounting to a breach of the processing rules, and
- 8) the obligations of the certifier referred to in 42 and 43 GDPR, the obligations of the monitor referred to in 41(4) GDPR

	Controller	Sector	Country	Fine [€]
1	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746,000,000
2	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405,000,000
3	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225,000,000
4	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90,000,000
5	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000
6	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000
7	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50,000,000
8	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708
9	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	27,800,000
10	Enel Energia S.p.A	Transportation and Energy	ITALY	26,500,000

G+P Compensation - GDPR 82

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. - **PRINCIPLE**
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. - **PROCESSOR**
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. - **PRINCIPLE**
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 – **JOINT LIABILITY**
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 - **COOPERATION**

Responsibility for:

- Adequate standard of data protection (32 GDPR) - Processor is accountable to the supervisory authority as well as to the data subjects whose data it processes on behalf of the Controller
- Legality of the Controller's instructions
- Documenting the Controller's instructions
- Data misappropriation = „marching” into the Controller's sphere of authority

The GDPR does not differentiate between a „direct processor” and the "sub-processor" - 28.2 and 28.4 talk about "other processor" = **liability along the entire processing chain**

Article 34 GDPR

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach

If the communication to a data subject would involve disproportionate effort, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

- **Cost of incident investigation** - e.g., the cost of an outside law firm conducting an audit of the incident
- **Cost of incident notification**
- Cost of notifying those whose data has been breached

Liability for non-compliance with GDPR

A. PERSONAL

- General **criminal**
- **Criminal** obstruction
- **Staff**, including
- **Disciplinary**

B. Controller RESPONSIBILITY

- **Reputational**
- **Business** (contractors)
- **Financial**
- **Civil**: GDPR, tort, contractual
- **Administrative**

Division of roles in the organization

Role and responsibility of the DPO

DPO and compliance

When should there be a DPO?

37(1) GDPR

- a) public authority or body ...the courts too
- b) main activity = processing operations requiring **systematic monitoring** on a large scale
- c) main activity = processing of special categories of data and criminal data on a large scale

What if you don't need a DPO?

Document your analysis of the lack of obligation to appoint a DPO. ...Accountability / WP29 Guidelines

Who can be DPO?

Article 37(6) GDPR

- staff (employee, personal service provider)
- company (outsourcing)

Criteria for selecting the DPO

- professional qualifications, expertise, ability to carry out the tasks referred to in Article 39
- in-depth knowledge of GDPR, knowledge of local and EU data protection legislation
- sectoral knowledge, knowledge of organisations
- IT knowledge
- cybersecurity expertise
- ability to promote a data protection culture in the organization
- regular training

Article 38.6 GDPR

- management and other substantive positions (decision-making on objectives or means)
- WP 29
- organisational conflict (cross-subordination)
- substantive conflict (crossing of duties)
- time conflict (cross availability)
- DPO vs head of compliance or internal audit in a large company? Better not (substantive conflict + time conflict)

Art. 38 par. 3 sentence 1 GDPR

"The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. (...)"

- The DPO is not bound by instructions from the Controller, including indications of, for example, the interpretation of the provisions of the GDPR;
- Controller partner/advisor relationship.

- Prohibition on the dismissal and sanctioning of DPOs

In accordance with Article 38(3), second sentence, of the GDPR the DPO

"(...) shall not be dismissed or penalised by the controller or the processor for performing his tasks. (...)"

- The prohibition also includes revocation and punishment when refusing to comply with an order of the controller.

WP 29 :

- Lack of or delay in promotion (how to promote a DPO?!), impediment to professional development (denial of training), restrictions on access to benefits offered to other employees (discrimination).
- It means DPOs can't be temporarily delegated to other tasks, such as manning the printer in the hallway, much less assurance duties ;-)

- A cancellation should be understood as a termination of an employment contract or a service contract - outsourcing!
- WP 29 only gives reasons for discipline
e.g. theft, physical and mental harassment, sexual harassment, gross misconduct

How do you normally fire a DPO?

- Demonstrate that one is ignorant, lacks emotional intelligence (antagonistic personality), lacks training
- You can't revoke the DPO because the organization got a penalty
- Better to hire for a definite period

- Direct reporting to the Board.

In accordance with Article 38(3) sentence 3 of the GDPR:

"(...) The data protection officer shall directly report to the highest management level of the controller or the processor."

- It gives you the opportunity to directly report violations, information about non-compliance with the DPO's recommendations, submit your opinions and reports.
- The DPO is to be assured of being heard.

Tasks of the DPO - Article 39(1) GDPR

- information, education, sensitization, training
- knowledge audits
- monitoring and compliance audits
- recommendations and monitoring of the DPIA
- cooperation with supervisory authority

G+P Responsibilities of the DPO

- The DPO **is not responsible** for the organization's data protection compliance
- The responsibility still lies with the management
- So, let the management should appoint another person responsible for data protection other than the DPO

- The DPO should not act as a compliance officer
- DPOs and compliance are supposed to work together
- The DPO is part of the organization's compliance but does not report to the compliance officer and reports to management
- Compliance cannot control the DPO in the performance of the DPO function - independence of the DPO
- Compliance can verify "GDPR compliance" and assess risks

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

The principle of consent
Christina Panagoulea

Athens, 14 October 2022



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

1. A useful tool for data protection

- Data is undoubtedly the fuel of the digital economy and the fourth industrial revolution. International and EU legislation is required to safeguard the **right of informational self-determination**. This right consists of the individual's control over the management of the flow of information concerning him/her, as well as the possibility of separating publicly available information from private information, the disclosure of which to specific recipients depends on the will and consent of the individual.
- The individual is the one who can allow intervention in his private sphere. The institution used for the voluntary intervention in general in the legal tools of the individual is that of consent. **Consent** is a useful tool of data protection as it ensures the person's participation in the decisions concerning the use of his/her data, maintaining the central principle of the right of informational self-determination.
- **Directive 95/46/EC:**
 - Provided consent is still valid to the extent that it is consistent with the Regulation.
 - New technologies to ensure compliance, otherwise processing must be stopped.

2. Consent's anatomy

The **definition** of consent according to article 4 point 11) of GDPR:

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

- **Elements of valid consent:**

- Indication of will (legal nature)
- Freely given (imbalance of power, conditionality, granularity, detriment)
- Specific
- Informed
- Unambiguous indication of wishes

2.1 Legal nature of consent

- Two conceptual elements:

- **Indication & Will**

- A unilateral and addressable declaration of intent
- A form of authorization to someone (data controller) to intervene in the legal sphere of the authorizer (data subject).



2.2 Free/freely given

- Real choice, real control, should not be provided by a defective will of data subject.
- Must not be combined with a non-negotiable part of the terms and conditions.
- No pressure or influence on the subject.

2.2 Free/freely given-Imbalance of power

- **Public authorities**

Recital No. 43: *In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller **is a public authority** and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. [...].*

- **Employment**

It is almost unlikely that an employee will be able to freely respond to an employer's request for consent to, for instance, the activation of surveillance systems such as workplace camera surveillance –to the extent it is allowed- without feeling pressured to provide consent of (A.88 and Recital No. 155).

2.2 Free/freely given-Conditionality

- Consent that is not necessarily associated with the performance of a contract or the provision of services cannot be presented/claimed by controllers as a mandatory consideration/prerequisite for the contract/service. There should be a direct and objective link connection (of necessity) between the processing and the purpose of the execution.

2.2 Free/freely given-Granularity

- Recital No. 43

*[...] Consent is presumed not to be freely given if it does not allow **separate consent** to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*

- The subject should not be required to consent **to all purposes** (when the controller have combined multiple purposes) but should be given the option to be included separately. Otherwise, he/she has not freely consented. So detailed analysis means separation of purposes and obtaining consent for each individual purpose.

2.2 Free/freely given-Withdrawal or Refuse without Detriment (1/2)

- Recital No. 42:

*Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (1) a declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and **it should not contain unfair terms**. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. **Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.***

2.2 Free/freely given-**Withdrawal or Refuse without Detriment (2/2)**

- It follows from recital No. 42 of GDPR, that controllers in all cases must prove that if the subject does not consent or withdraws consent, he/she will not suffer a loss. Such harm exists when withdrawing consent entails costs. Other types of damage are deception, intimidation, coercion, degradation of the performance of the service at the expense of the data subject or significant negative consequences.

2.3 Specific

- Pursuant to Article 5(1)(b) GDPR (**purpose limitation principle**), obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.
- Determination of purpose & granularity in consent request are safeguards against “**function creep**” (gradual widening or blurring of purposes after a data subject has agreed to the initial collection of the data) which creates a risk of unexpected data usage and loss of subject's control over its data.
- **Consent mechanisms** must be detailed, specific and responsive to the subject's free consent. If the controller requests consent for more than one purpose, there should be a separate option for each purpose.

2.4 Informed consent (1/2)

- According to **Guidelines 05/2020** of European Data Protection Board (EDPB), the minimum content requirements of the information re consent are the followings :
 - a) identity of controllers
 - b) purpose of each data process for which consent is requested
 - c) the type of data that will be processed.
 - d) the existence of the right to withdraw consent
 - e) the information for automated individual decision-making based on 22 par. 2c of Regulation and
 - f) the information (according to articles a. 46 + 49 par. 1a) on potential risks of data transmission due to the absence of an adequacy decision and appropriate guarantees.
- These guidelines **are not binding** and should be **adjusted** specifically in special cases where more information may be needed to allow the data subject to genuinely understand the processing operations at hand.

2.4 Informed consent (2/2)

- **How** to provide information:
 - It can be made by written or oral declaration with audio or visual messages, in an understandable for the average person way and not hidden in general terms and conditions.
 - According to the EDPS, a controller must assess **what kind of audience** it is that provides personal data to their organization (are the minors? If yes, information must be understandable. After identifying their audience, controllers must determine **what information** they should provide and, subsequently **how they will present** the information to data subjects.
 - Consent request should be **distinct** or even on a **separate** form and cannot be contained in paragraph among/in the terms and conditions.

2.5 Unambiguous indication of wishes (1/3)

- Consent should constitute an overt, positive (not passive) action or statement and not an implied or presumed or conjectured one. This element of consent requires that the data collectors should use mechanisms that leave no room for doubt as to subject's intention to consent. The provision of consent must precede the start of processing (A. 6 par. 1a GDPR) .
- What is **not** an active indication of consent:
 - the pre-filled box, silence or inactivity and the simple use of the provided service. It is also not valid to provide consent embedded in a contract agreement or in general terms and conditions of service.

2.5 Unambiguous indication of wishes (2/3)

- **Online environment:**

- The consent request submitted by electronic means must not unreasonably disrupt the use of the service (user's experience). The consent mechanism should be **distinct** from other actions. This was also decided by the Hellenic Data Protection Authority (HDPa) with its decision No. 66/2018, where it ruled that the simple acceptance of messages from controllers does not constitute consent.

- **Selection of desired settings**

- Another way of giving consent specifically in the Information Society, as in the Social Media Platform, e.g., Instagram, is the selection of desired settings (recital paragraph 32). But this is problematic because Instagram and other platforms set, by default, the user's profile to be publicly accessible, using an opt-out system. The user is often not informed about this setting, unless he/she looks at the settings himself/herself, in order to find out. Therefore, how can this “by default settings” be considered unambiguous indication of wishes ?

(3/3)

- **Case C-61/19** before the Court of Justice of the European Union (CJEU)
 - Orange Romania (telecommunication service provider) had included clauses in the contracts, in the form of **pre-filled boxes**, among which was the one regarding the customer's information **and consent** to the storage of copies of identity documents containing personal data, for identification purposes.
 - **Decision:** A contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes **is not such as to demonstrate that that person has validly given his or her consent**, as provided for in those provisions, to that collection and storage, where the box referring to that clause **has been ticked** by the data controller before the contract was signed, or where the terms of that contract are capable of **misleading** the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or where the **freedom to choose to object** to that collection and storage is unduly affected by that controller in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal.
 - The decision will have an **impact** on all service providers who rely on standardized and pre-populated consent clauses. Each service provider must be able to demonstrate that their customers have freely given their consent and that they have not used deceptive practices to obtain valid consent. CJEU's emphasis on free and informed consent establishes the important link between data protection and consumer law, as the decision recognizes the role of transparency and the potential for misleading practices when seeking consent.

3. Mandatory explicit consent

1. Processing of **special categories of personal data** (A. 9)
 2. In **automated individual decision-making**, including profiling (A. 22) and
 3. In the **transmission** to third countries or international organizations in the absence of appropriate guarantees (A. 49).
- The term "explicit" assures controllers themselves that there will be no doubt and potential lack of evidence in the future. The Regulation does not require consent to be given in writing form, but it can also be given by an e-mail statement, by clicking on a pop-up window, a scanned form bearing the data subject's signature or even an electronic signature. It can also be provided orally, such as by recording, as long as the information is objective, understandable and clear and as long as specific confirmation has been requested, such as by pressing a button or providing verbal confirmation.

3. Mandatory explicit consent-Special categories of personal data

- Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as “special categories” of personal data. The special categories are, for instance, personal data revealing racial or ethnic origin, genetic data and biometric data processed for the purpose of uniquely identifying a natural person and data concerning health.
- Article 9(2) does not recognize “necessary for the performance of a contract” as an exception to the general prohibition to process special categories of data. Therefore, controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) (b) to (j) e.g. establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity, vital interests of a person, processing relates to personal data which are manifestly made public by the data subject, legitimate interests of company/organization etc. Should none of the exceptions (b) to (j) apply, **obtaining explicit consent** in accordance with the conditions for valid consent in the GDPR remains **the only possible lawful exception** to process such data.

3. Mandatory explicit consent-Case of Clearview in Greece and the HDPA Decision

- The US-based company “Clearview AI Inc” has as its unique product **facial recognition platform**, which allows users (usually police agencies) to match **photos** found online through “web scraping”, i.e., the non-geographic collection of images and videos containing human faces from social networks (Facebook, YouTube etc.), as well as **information** extracted from the images and videos, such as geographic location metadata and **stored in its database**. The elicited face is converted into a numeric sequence and hashed in order to create a list and also identify future faces.
- It falls under the provisions of article 4 paragraph 4 of the Regulation where **profiling** means any form of automated processing for the evaluation of certain aspects of a natural person.
- Subjects are likely to **never learn** that their data has been processed except by accident if they read a publication about the company's practices.
- HDPA (**decision no. 35/2022**) considered not only that the data subject (Homo Digitalis NPO, the complainant) has not provided any consent but also ruled that it would not be possible for the data subject - based on the characteristics of the processing in question- **to provide consent at all**. Violating therefore the basic principles of legality of the processing (A. 5,6,9), the potentially high number of subjects located in Greece that are affected, the processing of a special category of data (biometrics) without any of the cases of 9 par. 2 , the Authority ruled that such process was illegal and **imposed a fine** of 20 million euros.

4. Additional conditions for obtaining valid consent-Demonstrate consent (1/2)

- Recital No. 42:

*Where processing is based on the data subject's consent, the controller **should be able to demonstrate** that the data subject has given consent to the processing operation. [...]*

Article 7 par. 1:

*Where processing is based on consent, the controller **shall be able to demonstrate** that the data subject has consented to processing of his or her personal data.*

- The controller should demonstrate, by keeping records of how and when he/she was informed, that all conditions of valid consents are met, that valid consent has been provided even after the processing activity has been completed.
- If the processing operations change or evolve significantly, the initial consent is not valid and a new one should be requested.
- This is the case, where consent is the only legal basis for data processing.

4. Additional conditions for obtaining valid consent-**Demonstrate consent** (2/2)

- HDPa issued **Directive 02/2011** proposing **technical measures on electronic consent** to the processing of personal data for the purpose of communications (SMS, email, fax, voice mail etc). For example, for a valid consent to be ensured, the user must before reach through the scroll bar to the end or correspondingly, declare his consent in a pop-up window which will include the text of the update.
- Although these techniques have been widely accepted by the controllers, in practice it is disputed whether the subject receives knowledge of the terms of the declaration of consent. When someone wishes to use an online service and is asked for electronic consent, they will rarely go through the process of reading the terms and conditions.

4. Additional conditions for obtaining valid consent-**Withdrawal of consent**

- Article 7 par. 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.

- Withdrawal of consent should be able to occur as easily as provided and not necessarily in the same way.
- Withdrawal should not entail damage/negative impact that may consist of both additional costs and a reduction in the level of service.
- The processing operations until the valid withdrawal remain lawful.

5. Processing in the context of employment (1/3)

Article 88 GDPR

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules **to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context**, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

5. Processing in the context of employment (2/3)

- The fulfillment of the conditions of article 7 of the GDPR for the legality of consent **constitutes a condition of the legality of the processing** and the corresponding decisions of the employer.
- **Opinion No. 2/2017 of Working Group 29:** Employers must respect the fundamental principles of data protection, regardless of the analog or digital technology. It is pointed out that consent is highly unlikely to constitute a legal basis in the case of employment unless employees can refuse without suffering adverse consequences.
- **Guidelines on transparency under Regulation 2016/679 of Working Group 29 :** If the processing is not necessary for the performance of the contract, such processing takes place lawfully only if is based on another appropriate legal basis.

5. Processing in the context of employment (3/3)

- **Greek Law 4624/2019 for the implementation of the GDPR provides that:**
 - *Article 27 par. 2. If the processing of an employee's personal data exceptionally has as a legal basis his/her consent, for the judgment that this was the result of free choice, the following must be considered: a) the employee's dependence existing in the employment contract and b) the circumstances under which consent was granted. The consent is given either in written or electronic form and must be clearly distinguished from the employment contract. The employer must inform the employee either in writing or electronically about the purpose of the processing of personal data and their right to withdraw consent in accordance with Article 7(3) of the GDPR.*
- The Greek law sets two specific requirements to establish the validity of the employee's consent:
 - a) the employee's **dependence** on the employer existing in the contract and b) the **circumstances** under which it is provided.
 - These two criteria constitute, according to the explanatory statement of the law, an indicator for judging whether the consent provided by the employee is a product of free choice or not, something that will ultimately be judged ad hoc by the Authority and/or by the Courts

5. Processing in the context of employment- Decision No. 12/2022 of HDPA (1/3)

- The employer was continuously monitoring the teacher's/employee's courses provided online in order to evaluate the quality of teaching services provided by the employees.
- The employee (complainant) points out that **she never consented** to the said monitoring of her online courses, that she expressed her **explicit objection** and proposed alternative ways as milder means. She also claimed that she was never **informed** about the type of personal data collected, about the purposes of the processing, about who has access to this data as well as about her right to access to the data concerning her.

5. Processing in the context of employment- Decision No. 12/2022 of HDPA (2/3)

- The employer claims that the complainant was aware of the Privacy Policy of her tutoring school but due to her own negligence **the employee did not sign** the statement of consent as the other employees did. The employer further claims that the employee subsequently consented to written messages addressed to her by the employer. The employer also refers to the complainant's **indirect and presumed consent** to the processing. The employer additionally invokes “the performance of a contract” (A.6 par.1b GDPR) as the legal basis for data processing.

5. Processing in the context of employment- Decision No. 12/2022 of HDPA (3/3)

- The HDPA concluded that valid consent was not proven. It is noted that even if the employer **infers** the complainant's consent to the processing, this does not constitute “valid” consent because consent must be expressed in a way that there is **no doubt or ambiguity** as to the intention of the person whose consent was provided.
- The Authority also stated that such “consent”, as the one claimed by the employer, cannot be considered a legitimate legal basis in data processing. Consent is not valid because it is not freely provided, when there is actual or potentially relevant harm resulting from the non-grant of consent.
- The **ambiguity** that was created by the employer, **regarding the legal basis** of processing deprives the Authority of the possibility control of the correctness of the choice of legal basis thereby violating the principle of accountability. The authority imposed an **administrative fine** on the employer.

5. Processing in the context of employment-

Lopez Ribalda vs Spain (1/2)

- Case of the European Court of Human Rights (ECtHR)
 - Supermarket workers were fired because they were caught stealing by **hidden cameras**, for the existence of which they were not informed. After their dismissal (having admitted the theft), the workers appealed to the Spanish courts asking their dismissal to be annulled, as illegal, because it was based on evidence material that came from the invasion of their privacy.
 - The **Spanish courts rejected** their lawsuit and the workers appealed to the ECtHR, which initially vindicated them, but referred the case to the Plenary, due to its importance.

5. Processing in the context of employment- **Lopez Ribalda vs Spain (2/2)**

- On the one hand, there is the right to protect the employer's property and on the other hand the right to protect private life.
- The Court ultimately ruled that **there was no infringement** of the right to privacy of the employees and that the Spanish courts properly weighed and balanced the rights of the employees and those of the employer and that they properly considered the justification provided by the company-employer for the use of the hidden camera.
- **But preventive monitoring** to ensure the protection of property should not be carried out in a way in which everyone without exception has their data processed in the workplace - because in addition to the employees who committed theft, **law-abiding workers were also monitored without exception.**
- As Judge Dedov specifically stated, the right to private life should never be used as an **alibi** for committing criminal acts.

6. Children (1/5)

- **Recital No. 38 GDPR**

Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

- **Article 8 GDPR**

*1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is **at least 16 years** old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.*

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

6. Children (2/5)

- Article 21 of the Greek implementing law 4624/2019
 - Par. 1. *When Article 6(1)(a) of the GDPR applies, the processing of personal data of a minor, when offering information society services directly to him (creating an Instagram account), is lawful, as long as the minor has reached the age of **15 year of age** and provides his consent.*
 - Par. 2. *If the minor is under 15 years of age, the processing of paragraph 1 is lawful only after the consent of his legal representative.*
- The Greek legislator, using the “flexibility” provided by article 8 of the GDPR, determines the age limit of “digital adulthood” for minors, as a vulnerable social group, who can validly provide their consent, at the age of 15.

6. Children (3/5)

- When consent is requested for the processing of children's personal data in the context of providing Information Society services directly to children, then the provision of **consent is valid only when it is provided by minors over 16 years old**. Otherwise, only when the person **exercising parental care** approves or gives consent himself/herself.
- To ensure the "**fully informed**" consent of a minor, the controller should consider the target audience, the method and language of informing (simple and clear).

6. Children (4/5)

- In cases where the parent or carer needs to give **consent or approve** consent, then a set of information may be required to achieve 'fully informed' decision
- It is understood that when the child reaches the **required age or becomes an adult**, he/she can withdraw, modify or confirm the consent.
- If the consent was provided on his/her behalf by the person exercising parental care, when he/she reaches the required age or becomes an adult, it does **not** mean that the consent **will cease to exist** by itself.

6. Children (5/5)

- The GDPR shifts the **burden of proving** that the conditions for the processing of the minor's personal data are met on the controller, who, within the framework of the principle of accountability established by the Regulation, must make **reasonable efforts** to verify that consent is given or approved by the person who has parental care of the child, considering available technology (parental control software).
- Relevant **technical measures** should be taken to verify the age of the child through checks both for the protection of the child and to ensure compliance with the legality for the controllers themselves, especially in cases where the child misrepresents his/her age.
- The technological parameterization of the controllers' systems should be obtained after checking the **national deviations** regarding the legal age of participation of minors (e.g. geographical localization of users in order to establish whether the user who is a minor lives for example in Greece)

7. Scientific Research (1/2)

Recital No. 159

*Where personal data are processed **for scientific research purposes**, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.*

7. Scientific Research (2/2)

- Where consent is the **legal basis** for processing to conduct research, this consent should be separated from other consent requirements that act as an ethical standard or procedural condition, such as clinical trials.
- When it is **not possible to specify** the context of the scientific research, according to Recital No. 33 the possibility-exception is provided to describe the purpose at a more **general level**. As a trade-off, consent may be sought at the outset for a broader context, but as it evolves, **a new consent** should be sought again prior to each stage.
- It is important that data subject is **informed** of the purposes and of his rights, especially that of revocation. It is pointed out by the EDPS that this "flexible approach" should be interpreted restrictively when it concerns data of special categories.

8. Cookies (1/4)

According to article 5 par. 3 of the e-Privacy Directive (2005/58), as was amended by Directive 2009/136/EC, the storage of information or access to already stored information on the terminal equipment of the subscriber/ user, is lawful **only when** the latter has given his/her **consent in advance**, based on clear and extensive information through the cookie policy.

8. Cookies (2/4)

In case **C-673/2017**, the CJEU ruled that the consent of article 2 paragraph f and article 5 paragraph 3 of Directive 2002/58 in combination with article 2 paragraph h of Directive 95/46 is not validly given when the storage of information or access to information already stored on the website user's terminal equipment, through cookies, is allowed based on a **pre-filled box** by the service provider, which the user must deselect in order to refuse to give consent.

8. Cookies (3/4)

- In the **guidelines No. 02/2013** (Working Party 29) elaborates that should a website operator wish to ensure that a consent mechanism for cookies satisfies the conditions in each Member State such consent mechanism should include each of the main element's specific information, prior consent (before the data processing starts, before cookies are set or read) indication of wishes expressed by user's active behavior and an ability to choose freely.

8. Cookies (4/4)

- Most cookies are personal data, and their process usually requires the express consent of the data subject (internet user). Accordingly, they **do not constitute personal data** and therefore **do not require consent**, since technically they do not lead to the identification of the user, only the cookies that are used once and temporarily per session or for the technical support of the connection (session cookies, user input, authentication).

9. Unsolicited communications

(1/3)

Article 11 of Greek Law 3471/2006 + Article 13 of Directive 58/2002

Par. 1: *The use of automatic dialing systems, in particular using facsimile (fax) or e-mail devices, and in general the making of unsolicited (even initial ones with the purpose of prompting a declaration of consent) communications by any means of electronic communication, without human intervention, for the purposes of direct commercial promotion of products or services and for any kind of advertising purposes, is only permitted if the subscriber expressly consents in advance.*

Par. 2: *Unsolicited communications with human intervention (calls) are not allowed for the above purposes, if the subscriber has declared to the provider of the service available to the public, that he does not wish to receive such calls in general.*

Par. 3: *Email contact details obtained legally, in the context of the sale of products or services or other transaction, may be used to directly promote similar products or services of the supplier or to serve similar purposes, even when the recipient of the message has not given their consent in advance, provided that he is provided in a clear and distinct way with the possibility to object, in an easy way and free of charge, to the collection and use of his electronic data and this during the collection of contact data, as well as in every message, in the event that the user he had not originally objected to this usage.*

9. Unsolicited communications

(2/3)

- Phone calls with **human intervention** are allowed, unless the called party has indicated that it does not want them. These registers are called “opt-outs”.
- Especially **for automated calls**, in case that the data subject is not registered in the opt-out register, prior consent is a prerequisite.
- An opt-out register similar to the abovementioned is "Register of Article 13" of the HDPA, that includes natural persons who have **declared** that they do not wish to receive communication via traditional mail on matters concerning the promotion/advertisement of goods. Controllers are required to consult the register and delete from their lists those registered in it. This register does not apply to electronic communications (eg telephones, SMS, email).

9. Unsolicited communications (3/3)

- **No. 1343/2022 decision of the Council of State (High Administrative Court)** **annulled** the decision of the HDPa, which imposed a fine on a member of parliament, who carried out unsolicited political communication via short messages (SMS), in the context of promoting his candidacy in the parliamentary elections without providing the data subject with the possibility to exercise the right to object and without having any relationship with the complainants.
- According to the Council, political communication was incorrectly equated with advertising activity limiting the applicant's ability to participate in the political life of the country.

Final thoughts (1/2)

- There is not enough room for negotiation, as the user is asked to consent only based on standardized privacy policies and is therefore faced with a “take it or leave it” situation.
- Data Subject has no choice but to consent since there are no alternatives to the quasi-monopoly online platforms.
- Users are increasingly dependent on the use of these platforms, making their online existence dependent on the use of online platforms.
- The lack of free consent is due to the imbalance of power between users and platforms.

Final thoughts (2/2)

- The reality is that users do not read the privacy policy terms. It takes a lot of time (information overload) and the information the data subject is asked to read and understand is a lot (consent overload).
- Average user accepts the terms by giving their consent blindly.
- It is argued that terms and conditions of consent are not comprehensible to the average user. This is due to the legal language that is inevitably used in order to achieve the most complete information possible, ultimately leading to a paradox, because simplifying the text of the terms inevitably leads to a loss of information.
- Consent is not a “panacea” to the process of personal data.
- May God and ourselves protect us all from frivolous and frivolously given consent!

Thank you very
much!

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

**Data controller and processor
Evangelia Vagena**

Athens, 14 October 2022



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

Why are these concepts important?

- ❖ Crucial role in the application of the GDPR

They determine:

- who shall be **responsible for compliance** with data protection rules
- how data subjects can **exercise their rights** in practice

They are:

- ❑ **functional** concepts in that they aim to allocate responsibilities according to *the actual roles* of the parties and
- ❑ **autonomous** concepts in the sense that they should be *interpreted mainly according to EU data protection law*

➤ GDPR- Directive 95/46/EC:

- the concepts of controller and processor **have not changed**
- the **criteria** for how to attribute the different roles **remain the same**

*! the concept of 'controller' was essentially taken
from the Council of Europe's Convention 108 concluded in 1981!*

Ar. 4, 24-28 GDPR & Reference documents

- ▶ EDPB, [*Guidelines 7/2020 on the Concepts of Controller and Processor in the GDPR*](#) (2021).
- ▶ Article 29 Working Party, [*Opinion 1/2010 on the concepts of “controller” and “processor”*](#) (2010).

Controller & accountability principle I

The GDPR, in Article 5(2), explicitly introduces the accountability principle which means that:

- *the controller* shall be responsible *for the compliance* with the principles set out in Article 5(1) GDPR; and that
- *the controller* shall be able to *demonstrate compliance* with the principles set out in Article 5(1) GDPR.

=The aim of incorporating the accountability principle into the GDPR and making it a central principle was to emphasize that data controllers must implement appropriate and effective measures and be able to demonstrate compliance

“As the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, the concept of ‘controller’ should be interpreted in a sufficiently broad way,

favouring as much as possible effective and complete protection of data subjects so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules, while at the same time not diminishing the role of the processor.”

*EDPB, [Guidelines 7/2020 on the Concepts of Controller and Processor in the GDPR](#) (2021)

Controller & accountability principle II

The accountability principle is directly addressed to the controller.

However, some of the more specific rules *are addressed to both controllers and processors*, such as the rules on supervisory authorities' powers in Article 58.

Both controllers and processors:

- can be **fined** in case of non-compliance with the obligations of the GDPR that are relevant to them and
- are **directly accountable** towards supervisory authorities by virtue of the obligations to maintain and provide appropriate *documentation* upon request, *co-operate* in case of an investigation and *abide* by administrative orders.

Definitions

Article 4

Definitions

► For the purposes of this Regulation:

(7) **‘controller’** means

- 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;

where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) **‘processor’** means

- a natural or legal person, public authority, agency or other body
- which processes personal data **on behalf of the controller**;

Controller: “a natural or legal person, public authority, agency or other body”

- ▶ No limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.
- ▶ In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller
- ▶ Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller
- ▶ In principle, any processing of personal data by employees which takes place within the realm of activities of an organisation may be presumed to take place under that organisation’s control. In exceptional circumstances, however, it may occur that an employee decides to use personal data for his or her own purposes, thereby unlawfully exceeding the authority that he or she was given. (e.g. to set up his own company or similar)

Controller: “decides” I

- ▶ It refers to the controller’s influence over the processing, by virtue of an exercise of **decision-making power**.
- ▶ A controller is a body that decides certain key elements about the processing.
- ▶ Analysis of the factual elements or circumstances of the case

“why is this processing taking place?”

“who decided that the processing should take place for a particular purpose?”

Controller: “decides” II

Control stemming from legal provisions

Article 4(7) states that “where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its *nomination may be provided for by Union or Member State law.*”

When the law establishes a task or impose a duty on someone to collect and process certain data

Example: Legal provisions

The national law in Country A lays down an obligation for municipal authorities to provide social welfare benefits such as monthly payments to citizens depending on their financial situation. In order to carry out these payments, the municipal authority must collect and process data about the applicants’ financial circumstances. Even though the law does not explicitly state that the municipal authorities are controllers for this processing, this follows implicitly from the legal provisions.

Control stemming from factual influence

The need for factual assessment means that the role of a controller does not stem from the nature of an entity that is processing data but from its **concrete activities** in a specific context. The same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity

Certain processing activities can be considered as naturally attached to the role or activities of an entity ultimately entailing responsibilities from a data protection point of view

Example: Providing an electronic communications service such as an electronic mail service involves processing of personal data. The provider of such services will normally be considered a controller in respect of the processing of personal data that is necessary for the operation of the service as such (e.g., traffic and billing data). If the sole purpose and role of the provider is to enable the transmission of email messages, the provider will not be considered as the controller in respect of the personal data contained in the message itself. The controller in respect of any personal data contained inside the message will normally be considered to be the person from whom the message originates, rather than the service provider offering the transmission service.

Controller: contractual arrangements of the identity of the controller

- ✓ If there is no reason to doubt that it *accurately reflects the reality*, there is nothing against following the terms of the contract.
- ✓ The terms of a contract are not decisive in all circumstances, as this would simply allow parties to allocate responsibility as they see fit.
- ✓ It is not possible either to become a controller or to *escape controller obligations* simply by shaping the contract in a certain way where the *factual circumstances* say something else.

Controller: “Alone or jointly with others”

- ▶ Several different entities may act as controllers for the *same* processing, with each of them then being subject to the applicable data protection provisions.
- ▶ see joint controllers provision

Controller: “Purposes and means” I

- ▶ Determining the purposes and the means amounts to deciding respectively the “why” and the “how” of the processing: given a particular processing operation, the controller is the actor who has determined why the processing is taking place (i.e., “to what end”; or “what for”) and how this objective shall be reached (i.e. which means shall be employed to attain the objective). A natural or legal person who exerts *such influence over the processing* of personal data, thereby participates in the determination of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR
- ▶ In practice, if a controller engages a processor to carry out the processing on its behalf, it often means that the processor shall be able to make certain decisions of its own on how to carry out the processing. Some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing. In this perspective, there is a need to provide guidance about **which level of influence** on the “why” and the “how” should entail the qualification of an entity as a controller and to what extent a processor may make decisions of its own.

Controller: “Purposes and means” II

As regards the determination of means, a distinction can be made between **essential** and **non-essential** means.

❑ “**Essential means**” are traditionally and inherently reserved to the controller. While nonessential means can also be determined by the processor, essential means are to be determined by the controller. “Essential means” are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed (“which data shall be processed?”), the duration of the processing (“for how long shall they be processed?”), the categories of recipients (“who shall have access to them?”) and the categories of data subjects (“whose personal data are being processed?”). Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate.

❑ “**Non-essential means**” concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.

Example: Bank payments

As part of the instructions from Employer A, the payroll administration transmits information to Bank B so that they can carry out the actual payment to the employees of Employer A. This activity includes processing of personal data by Bank B which it carries out for the purpose of performing banking activity. Within this activity, the bank decides independently from Employer A on which data that have to be processed to provide the service, for how long the data must be stored etc. Employer A cannot have any influence on the purpose and means of Bank B’s processing of data. Bank B is therefore to be seen as a controller for this processing and the transmission of personal data from the payroll administration is to be regarded as a disclosure of information between two controllers, from Employer A to Bank B

Controller: “Of the processing of personal data”

- ▶ It is **not necessary** that the controller **actually has access** to the data that is being processed.
- ▶ Someone who **outsources** a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data.

Controller- special obligation

Article 25 GDPR. Data protection by design and by default

“1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, **the controller shall**, both *at the time of the determination* of the means for processing and *at the time of the processing* itself, **implement appropriate technical and organisational measures**, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, *by default*, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. [...]”

Controller- special obligation

Article 25 GDPR. Data protection by design and by default – *in simple words*

- ▶ “Overall thrust of the provision” : impose an obligation on controllers to put in place technical and organisational measures that are *designed* to implement data protection principles and the rights of data subjects.
- ▶ The controller is responsible for adherence with these principles, but Recital 78 stipulates that producers of applications, products, and services, are *encouraged* to consider the data protection obligations that controllers need to fulfil. So, the goal is to have developers and controllers *embrace a culture of responsibility* and systematically indicate processes which could infringe the GDPR, and to strengthen the data subject's trust in the processing systems.
- ▶ In order to be effective, data protection must be implemented *ex ante*. Hence, the controller must define the privacy requirements that need to be taken into account while engineering, and determine the default settings of the final product

JOINT CONTROLLERS- the GDPR provision

► Article 26 GDPR. Joint controllers

1. Where two or more controllers **jointly determine** the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner **determine their respective responsibilities** for compliance with the obligations under this Regulation, in particular as regards the **exercising of the rights** of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of **an arrangement between** them unless, and in so far as, the respective responsibilities of the controllers are **determined by Union or Member State law** to which the controllers are subject. The arrangement may designate **a contact point** for data subjects.
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The **essence** of the arrangement shall be made **available to the data subject**.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation **in respect of and against each of the controllers**.

GDPR TOONS

COPYRIGHT 2017 B.DREYER GDPRTOONS.COM

PEOPLE ARE COMPLAINING TO
THE SUPERVISORY AUTHORITY THAT THEIR
DATA IS NOT BEING ERASED AS
REQUESTED!

WHICH ONE OF YOU
CONTROLLERS IS
RESPONSIBLE ??



INSPIRED BY:
S.KURT

JOINT CONTROLLERS- introduction

- ▶ the qualification of joint controllers will mainly have consequences in terms of **allocation of obligations for compliance** with data protection rules and in particular with respect to the rights of individuals.
- ▶ joint controllership exists with regard to a specific processing activity when **different parties determine jointly** the purpose and means of this processing activity
- ▶ Not all processing involving several entities give rise to joint controllership. The **overarching criterion** for joint controllership to exist is the joint participation of two or more entities in the **determination of the purposes and means of a processing**. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.

JOINT CONTROLLERS- the element of determination

- ▶ Usually, joint participation will take the form of a *common decision* (=intention) taken by two or more entities or result from *converging decisions* by two or more entities regarding the purposes and essential means
- ▶ Decisions can be considered as converging on purposes and means if they *complement* each other and are necessary for the processing to take place in such manner that they have a *tangible impact* on the determination of the purposes and means of the processing
- ▶ For example, in Jehovah's Witnesses [C-25/17], the CJEU considered that a religious community must be considered a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching.
 - ▶ The CJEU considered that it was not necessary that the community had access to the data in question, or to establish that that community had given its members written guidelines or instructions in relation to the data processing. The community participated in the determination of purposes and means by organising and coordinating the activities of its members, which helped to achieve the objective of the Jehovah's Witnesses community. In addition, the community had knowledge on a general level of the fact that such processing was carried out in order to spread its faith.
- ▶ The existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, the CJEU has clarified that those operators may be involved **at different stages** of that processing and to **different degrees so that the level of responsibility** of each of them must be assessed with regard to all the relevant circumstances of the particular case

JOINT CONTROLLERS- Jointly determined means I

- ▶ Two or more entities have *exerted influence* over the means of the processing.
- ▶ Also covers the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.
- ▶ The use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context.
 - ▶ **Example:** the CJEU held in *Wirtschaftsakademie* that the administrator of a fan page hosted on Facebook, by defining parameters based on its target audience and the objectives of managing and promoting its activities, must be regarded as taking part in the determination of the means of the processing of personal data related to the visitors of its fan page.
- ▶ The use of a **common data processing system** or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing).
 - ▶ **Example:** Travel agency A travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the travel agency, the airline and the hotel are three different data controllers processing the data for their own and separate purposes and there is no joint controllership.

JOINT CONTROLLERS- Jointly determined means II

► Example: Research project by institutes

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as *joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used* (the existing platform).

Each of the institutes however is a *separate controller* for any other processing that may be carried out *outside the platform* for their respective purposes.

JOINT CONTROLLERS- no joint controllership

- ❖ Not all kind of partnerships, cooperation or collaboration imply qualification of joint controllers as such qualification requires a **case-by-case analysis** of each processing at stake and the precise role of each entity with respect to each processing. The cases below provide non-exhaustive examples of situations where there is no joint controllership

- ▶ **Example:** Transmission of employee data to tax authorities

A company collects and processes personal data of its employees with the purpose of managing salaries, health insurances, etc. A law imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control. In this case, even though both the company and the tax authorities process the same data concerning salaries, the lack of jointly determined purposes and means with regard to this data processing will result in qualifying the two entities as two separate data controllers.

- ▶ **Example:** Marketing operations in a group of companies using a shared database

A group of companies uses the same database for the management of clients and prospects. Such database is hosted on the servers of the mother company who is therefore a processor of the companies with respect to the storage of the data. Each entity of the group enters the data of its own clients and prospects and processes such data *for its own purposes only*. Also, each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data. They cannot access or use each other's data. The mere fact that these companies use a shared group database does not as such entail joint controllership. Under these circumstances, each company is thus a separate controller.

PROCESSOR: DEFINITION

“a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller”=

- ▶ might be an *organisation*, but it might also be an *individual*
- ▶ Two basic conditions for qualifying as processor are:

- a) being a *separate entity* in relation to the controller and

Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot be a processor to another department within the same entity.

- b) processing personal data *on the controller's behalf*

In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means

It also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), *a processor infringes the GDPR* by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions

- ❖ obligations directly applicable specifically to processors

- ▶ A controller might also decide to engage one processor, who in turn - with the authorisation of the controller - engages one or more other processors (*“sub processor(s)”*)

PROCESSOR: examples

- ▶ **Example:** Service provider referred to as data processor but acting as controller

Service provider MarketinZ provides promotional advertisement and direct marketing services to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for other purposes than advertising for GoodProducts, *such as developing their own business activity*. The decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this set of processing operations and their processing for this purpose would constitute an infringement of the GDPR.

- ▶ **Example:** Taxi service

A taxi service offers an online platform which allows companies to book a taxi to transport employees or guests to and from the airport. When booking a taxi, Company ABC specifies the name of the employee that should be picked up from the airport so the driver can confirm the employee's identity at the moment of pick-up. In this case, the taxi service processes personal data of the employee as part of its service to Company ABC, but the processing as such is not the target of the service. The taxi service has designed the online booking platform as part of developing its own business activity to provide transportation services, without any instructions from Company ABC. The taxi service also independently determines the categories of data it collects and how long it retains. The taxi service therefore acts as a controller in its own right, notwithstanding the fact that the processing takes place following a request for service from Company ABC.

PROCESSOR OBLIGATIONS

- ▶ Main GDPR obligations for processors:
 - ▶ a processor must ensure that persons authorised to process the personal data have committed themselves to *confidentiality* (Article 28(3));
 - ▶ a processor must maintain a *record* of all categories of processing activities (Article 30(2)) and
 - ▶ must implement appropriate *technical and organisational measures* (Article 32).
 - ▶ A processor must also designate a *data protection officer* under certain conditions (Article 37) and
 - ▶ has a duty to *notify* the controller without undue delay after becoming aware of a personal *data breach* (Article 33(2)).
 - ▶ the rules on *transfers of data to third countries* (Chapter V) apply to processors as well as controllers.

Processor as a choice of the controller

- ▶ The controller has the duty to use “*only processors providing sufficient guarantees to implement appropriate technical and organisational measures*”, so that processing meets the requirements of the GDPR - including for the security of processing - and ensures the protection of data subject rights.
- ▶ The controller is therefore responsible for assessing the **sufficiency** of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration.
- ▶ The guarantees “provided” by the processor are those that the processor is able to demonstrate to the satisfaction of the controller, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations. Often this will require an **exchange of relevant documentation** (e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external data protection audits, recognised international certifications, like ISO 27000 series).
- ▶ The obligation to use only processors “providing sufficient guarantees” contained in Article 28(1) GDPR is a **continuous obligation**. It does not end at the moment where the controller and processor conclude a contract or other legal act. Rather the controller should, at appropriate intervals, verify the processor’s guarantees, including through **audits and inspections** where appropriate

RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR- see Data Processing Agreement I

- ▶ Any processing of personal data by a processor must be governed by a *contract or other legal act* under EU or Member State law between the controller and the processor
 - ▶ in writing, including in electronic form
 - ▶ the absence thereof is an infringement of the GDPR
- ▶ Other legal Act = such as a national law (primary or secondary) or other legal instrument.
- ▶ A written contract pursuant to Article 28(3) GDPR may be embedded in a broader contract, such as a service level agreement. In order to facilitate the demonstration of compliance with the GDPR, the EDPB recommends that the elements of the contract that seek to give effect to Article 28 GDPR be clearly identified as such in one place (for example in an *annex*).
- ▶ the controller and the processor may choose to negotiate their own contract including all the compulsory elements or to rely, in whole or in part, on *standard contractual clauses* in relation to obligations under Article 28.

Data Processing Agreement (DPA) Content

- ▶ the **subject-matter** of the processing (for instance, video surveillance recordings of people entering and leaving a high-security facility). While the subject matter of the processing is a broad concept, it needs to be formulated with enough specifications so that it is clear *what the main object of the processing* is;
- ▶ the **duration** of the processing: the *exact* period of time, or the *criteria* used to determine it, should be specified; for instance, reference could be made to the duration of the processing agreement;
- ▶ the **nature** of the processing: the *type* of operations performed as part of the processing (for instance: “filming”, “recording”, “archiving of images”, ...) and *purpose* of the processing (for instance: detecting unlawful entry). This description should be as comprehensive as possible, depending on the specific processing activity, so as to allow external parties (e.g. supervisory authorities) to understand the *content* and the *risks of the processing entrusted* to the processor.
- ▶ the **type of personal data**: this should be specified in the most detailed manner as possible (for instance: video images of individuals as they enter and leave the facility). It would not be adequate merely to specify that it is “personal data pursuant to Article 4(1) GDPR” or “special categories of personal data pursuant to Article 9”. In case of special categories of data, the contract or legal act should at least specify which types of data are concerned, for example, “information regarding health records”, or “information as to whether the data subject is a member of a trade union”;
- ▶ the **categories of data** subjects: this, too, should be indicated in a quite specific way (for instance: “visitors”, “employees”, delivery services etc.);
- ▶ the **obligations and rights of the controller**: the rights of the controller are further dealt with in the following slides (e.g. with respect to the right of the controller to perform inspections and audits).
 - ▶ As regards the obligations of the controller, examples include the controller’s obligation to provide the processor with the data mentioned in the contract, to provide and document any instruction bearing on the processing of data by the processor, to ensure, before and throughout the processing, compliance with the obligations set out in the GDPR on the processor's part, to supervise the processing, including by conducting audits and inspections with the processor.

RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR-III

- ▶ The processor must only process data on *documented instructions* from the controller (Art. 28(3)(a) GDPR)
 - ▶ this obligation stems from the fact that the processor processes data on behalf of the controller
- ▶ The processor must ensure that *persons* authorised to process the personal data have committed themselves to *confidentiality* or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR)
 - ▶ The broad concept of “persons authorised to process the personal data” includes employees and temporary workers
- ▶ The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR)
 - ▶ implement appropriate technical and organisational security measures
- ▶ The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR)
 - ▶ See sub processors
- ▶ The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the *data subject's rights* (Article 28(3) (e) GDPR).
 - ▶ the contract must stipulate that the processor has an obligation to provide assistance “by appropriate technical and organisational measures, insofar as this is possible”. The nature of this assistance may vary greatly “taking into account the nature of the processing” and depending on the type of activity entrusted to the processor

RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR-IV

- ▶ The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR)
 - ▶ the agreement should contain details as to how the processor is asked to help the controller meet the listed obligations
- ▶ On termination of the processing activities, the processor must, at the choice of the controller, *delete or return all the personal data* to the controller and delete existing copies (Art. 28(3)(g) GDPR)
 - ▶ it is therefore up to the controller to decide what the processor should do with regard to the personal data- delete them/return them?
- ▶ The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to *audits*, including *inspections*, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR)
 - ▶ include details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing that are relevant to demonstrate compliance
- ▶ Instructions infringing data protection law
 - ▶ The processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions
 - ▶ the processor has a duty to comply with the controller's instructions, but it also has a general *obligation to comply with the law*

Sub-processors

- ▶ the processor shall not engage another processor without *prior specific or general written authorisation of the controller* (including in electronic form).
 - ▶ In the case of **general written authorisation**, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In both cases, the processor must obtain the controller's *authorisation in writing before* any personal data processing is entrusted to the subprocessor
- ▶ If the controller chooses to give its **specific authorisation**, it should specify in writing which subprocessor and what processing activity it refers to. Any *subsequent change will need to be further authorised* by the controller before it is put in place. If the processor's request for a specific authorisation is not answered to within the set timeframe, it should be held as denied. The controller should make its decision to grant or withhold authorisation taking into account its obligation to only use processors providing "sufficient guarantees".
- ▶ Alternatively, the controller may provide its **general authorisation** to the use of sub-processors (in the contract, including a list with such sub-processors in an annex thereto), which should be *supplemented with criteria* to guide the processor's choice (e.g., guarantees in terms of technical and organisational measures, expert knowledge, reliability and resources). In this scenario, the processor needs to inform the controller in due time of any intended addition or replacement of sub-processor(s) so as to provide the controller with the opportunity to object
- ▶ Therefore, the main difference between the specific authorisation and the general authorisation scenarios lies in the **meaning given to the controller's silence**: in the general authorisation situation, the controller's failure to object within the set timeframe can be interpreted as authorisation.

CONSEQUENCES OF JOINT CONTROLLERSHIP I

- ▶ Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR
 - ▶ need to set “*who does what*”
 - ▶ ensure that where multiple actors are involved, especially in complex data processing environments, *responsibility for compliance with data protection rules is clearly allocated* in order to avoid that the protection of personal data is reduced, or that a negative conflict of competence lead to loopholes whereby some obligations are not complied with by any of the parties involved in the processing
 - ▶ The CJEU has recently stated that “*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*” [Wirtschaftsakademie, C-210/16]
- ▶ Allocation of responsibilities needs to be done by way of an arrangement
 - ▶ free to agree on the form of the arrangement- usually a contract
- ▶ The essence of the arrangement shall be made available to the data subject
 - ▶ For example, it must be completely clear to a data subject which data controller serves as a point of contact for the exercise of data subject rights (notwithstanding the fact that he or she can exercise his or her rights in respect of and against each joint controller).

CONSEQUENCES OF JOINT CONTROLLERSHIP II

- ▶ The arrangement may designate a **contact point** for data subjects
- ▶ Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers.
 - ▶ In case of joint controllers established in different Member States, or if only one of the joint controllers is established in the Union, the data subject may contact, at his or her choice, either the controller established in the Member State of his or her habitual residence or place of work, or the controller established elsewhere in the EU or in the EEA.
- ▶ Obligations towards data protection authorities
 - ▶ Joint controllers should organise in the arrangement the way they will **communicate** with the competent supervisory data protection authorities. Such communication could cover possible consultation under Article 36 of the GDPR, notification of a personal data breach, designation of a data protection officer
 - ▶ The authorities **can contact any of the joint controllers** to exercise their powers under Article 58 with respect to the joint processing.

Article 27 GDPR. Representatives of controllers or processors not established in the Union par. 1, 2

****“hidden obligation” of the GDPR****

«1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

[**ar. 3 (2) 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor **not established in the Union**, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.]

2. The obligation laid down in paragraph 1 of this Article **shall not apply to:**

(a) processing which is **occasional**, does not include, on a large scale, processing of special categories of data as referred to in *Article 9(1)* or processing of personal data relating to *criminal convictions* and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b) a **public authority** or body.

Article 27 GDPR

Representatives of controllers or processors not established in the Union par. 3-5

[...] 3. The representative shall be **established in one of the Member States** where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative **shall be mandated** by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be **without prejudice** to legal actions which could be initiated **against the controller or the processor» themselves.**»

Article 27 GDPR. Representatives of controllers or processors not established in the Union

*****in simple words***

- ✓ it applies to controllers and processors that are **not located in the EU** and are processing personal **data of data subjects in the EU** involving either the offering of goods / services or the monitoring of behavior happening in the EU. It does not apply to those organizations which have been established in the European Union and are within the scope of GDPR due to Article 3(1)
- ✓ a contact point in the European Union for the supervisory authorities and data subjects rather than require them to contact the company at its base of operations.
- ✓ The exceptions are cases where it is unlikely to result in a risk to the rights and freedoms of natural persons
- ✓ The representative must be **located** in one of the Member States where the data subjects who are **at the center of the processing** are located
 - ✓ E.g : if the personal data collected by a company only involves individuals in Paris, then the representative must be located in France. If personal data is collected from people in Germany and France, then the controller or processor can designate a representative in either country
 - ✓ Some non-EU companies may choose to create a subsidiary in the European Union to meet the representative requirement & fall in within Article 3(1) .
- ✓ The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under GDPR

Questions?



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

**The Directive 2016/680 – Personal data and criminal
offences and criminal penalties**

Georgios Yannopoulos

Athens, 14 October 2022

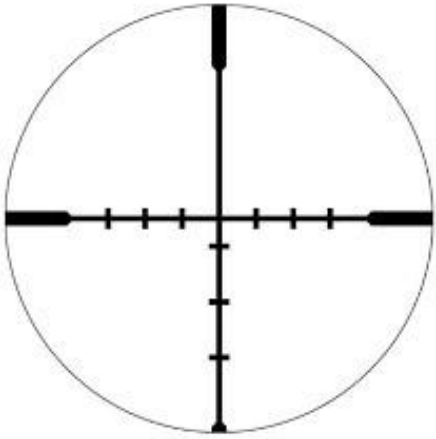


The project is co-financed with the support of the European Union's Justice programme

The Data Protection “package”

- **Regulation (EU) 2016/679 “GDPR” (27.4.2016)**
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)
[25 May 2018 / L. 4624/2019]
- **Directive 2016/680/EU / “Police or Law Enforcement Directive - LED” (27.4.2016)**
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
[6 May 2018 / L. 4624/2019]
- **Directive 2016/681/EU “Passenger Name Record – PNR” (27.4.2016)**
on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime
[25 May 2018 / L. 4579/2018]





680: Scope

applies to the processing of personal data by **competent authorities** (art. 3)
for **purposes** (art. 1):

- a) *prevention, investigation, detection or prosecution of criminal offences*
- b) *the execution of criminal penalties*
- c) *safeguarding against & prevention of threats to public security.*

competent authority (def. – 7):

- I) *Any public authority competent for (a), (b) or (c)*
- II) *any other body or entity **entrusted** by Member State law to exercise public authority and public powers for (a), (b) or (c)*

680: Structure I to V

I. General provisions

II. Principles

III. Rights of the Data Subject

IV. Controller & Processor

General Obligations

Security of PD

Data Protection officer

V. Transfers of PD to third countries (adequacy?)

680: Structure VI to X

VI. Independent Supervisory Authorities

VII. Cooperation

VIII. Remedies, Liability & Penalties

IX. Implementing Acts

X. Final Provisions



Obligations Identical with GDPR

gyannop@law.uoa.gr

Controllers

1. implement ATOM & demonstrate processing in accordance with Directive (19)
2. implement data protection *by design* and *by default* (20)
3. use Processors with sufficient guarantees & act only on instructions from Controller (22)
4. maintain a record of processing activities (24)
5. implement logging measures (25)
6. cooperate with the Supervisory Authority (26)
7. carry out a **data protection impact assessment** (when **high risk** to the rights and freedoms of natural persons - 27)
8. consult the supervisory authority in advance (cases listed in 28)
9. implement ATOM to ensure a level of security appropriate to the risk, especially for special categories of PD referred to in art. 10 (art. 29)
10. notify the supervisory authority for PD breach (72 hrs) when likely to result in a risk to the rights and freedoms of natural persons (30)
11. communicate the PD breach to the Data Subject without undue delay when breach is likely to result in a high risk to rights and freedoms (31)
12. designate a DPO according to art. 32
13. respect the conditions defined for the transfer of personal data to third countries or to international organizations (art. 35 and following).



Different Obligations of Controllers (specific to 680)

clear distinction between PD of different categories of data subjects (art. 6)

- convicted of a criminal offence
- victims of a criminal offence
- other parties to a criminal offence etc

distinguish between PD:

- based on facts / on personal assessments & ensure the quality of PD (art. 7)

processing must be lawful,

- necessary for the performance of a task carried out **by a competent authority**,
- for the purposes of this Directive, and based on Union law or Member State law (art. 8)

special categories: only where strictly necessary (art. 10)



Different Rights (specific to 680)

No right to portability

information to the data subject, subject to possible limitations (13)

right of access (14) subject to limitations in whole or in part:

- in order not to obstruct investigations
- to avoid prejudicing the prevention or detection of criminal offences, etc. (art. 15).
- "*indirect right of access*" → exercised through the intermediary of the competent supervisory authority (art. 17);

the right to rectification or erasure of personal data (16)



Greek Law Implementing 680 (L. 4624/2019)

Art. 2 (& art. 2 GDPR) contradicted by (arts. 43 & 84 L. 4624/19)

Art. 5 (time limits) not properly transferred (art. 73§4 L. 4624/2019)

Art. 8 (Lawfulness of processing) NOT transferred (purposes not specified)

- Also “consent” (art. 49 L. 4624) is not provided as legal basis in art. 8
- **680:** *“consent can only serve as a safeguard and cannot constitute the legal basis for such processing*

Art 10 (special categories) not properly transferred
(art. 46 L. 4624/2019)

Art. 11 Automated individual decision-making →
guarantees & measures not defined

What next?

Compliance: Mission  possible

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

Data transfers to third countries
Spyros Tassis

Athens, 14 October 2022



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

What is the issue here?

- Over the past three decades, data access, sharing and use have become central drivers of economic growth and social well-being. Data, and in particular their transfer and sharing across borders, have become an integral part of every sector of the economy as well as a critical source of innovation for disruptive technologies such as the Internet of Things and Artificial Intelligence. However, the ubiquitous exchange of data across borders has amplified a range of concerns for governments, businesses, and citizens, eroding trust among them.
- In response to this erosion of trust, policies and regulations addressing cross-border data flows are increasing. There are different reasons motivating countries to regulate cross-border data flows, often placing conditions on its sharing abroad. One reason is to safeguard the privacy of individuals and their personal data. Countries may also place conditions on the flow of data to ensure access by domestic authorities to data that are important for law enforcement or audit purposes. Conditions placed on cross-border data flows might also arise for the protection of information deemed to be sensitive from a security perspective. Lastly, some countries are using cross-border data regulation with a view to developing domestic capacity in digitally intensive sectors, as a form of digital industrial policy.

[OECD: CROSS-BORDER DATA FLOWS, October 2022]

What is the real issue here?

- Vast computing power combined with huge databases around the world
- Multinational companies that need to circulate data
- Numerous online services (cloud-based services)
- Data analytics (especially Google) that create added value information
- Data rights that need to be respected
- So how we ensure compliance?

Which activities are affected?

- Oh, all that data (the new fuel, the new money, the new economy etc.)
- AdTEch, Big Data, Analytics, cloud services, which are the new competition fields
- A market demand that drives (forces?) the regulatory necessity
- We have the first tools, but we need more regulatory certainty.
- Schrems decisions have increased pressure for better data transfer agreements but
- NOYB complaints against specific companies created a privacy arena.

Which activities are affected?

- The majority of content provided through Internet companies is offered at little to no cost, and consumers are accustomed to accessing information found on the Internet for free.
- The truth is that companies like Google, Meta (formerly Facebook), Yahoo, Twitter, and many others have various ways they can generate revenue while continuing to offer their unique web services at no cost to consumers.
- In 2021, Google generated more than 81% of its revenue from advertising and is diversifying its revenue by developing products and services in other industries, such as self-driving cars and cloud gaming systems.
- The main way these companies make money online revolves around monetizing data and selling ads.

What is the issue in the GDPR?

- **Article 44 GDPR** (General principle for transfers): Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.
- **Article 45 GDPR** (Transfers on the basis of an adequacy decision): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

What is the issue in the GDPR?

- **NO ADEQUACY DECISION** -> Article 46 (Transfers subject to appropriate safeguards)
- In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

BCRs, SCCs, Certifications etc

- When there is no decision for adequacy, we need other tools, i.e the derogations of Article 49 GDPR:
 - Binding Corporate Rules
 - Standard Contractual Clauses adopted by the Commission
 - Standard Contractual Clauses adopted by a supervisory authority and approved by the Commission
 - Approved code of conduct pursuant to Article 40
 - Explicit consent (!)
 - Approved certification mechanism pursuant to Article 42 (we now have the first decision of the EDPB)
- BCRs
 - pros: a single group policy which would apply to all entities and employees and in all jurisdictions.
 - cons: they must be approved by a DPA and that proved a really long and bureaucratic procedure.
- SCCs (C2C, C2P, P2P and P2C transfers)
 - pros: unified text with no need for prior approval since it is issued by the Commission
 - cons: do not cover third parties and public sector

BCRs, SCCs, Certifications etc.

- CJEU's ruling in Schrems II should be read in conjunction with the EDPB Recommendations 1/2020 (final adopted in June 2021) on supplementary measures when transferring personal data to third countries, which provides for a mandatory Transfer Impact Assessment (TIA), whereby the parties must assess the privacy risks of the data transfer taking into account the local laws and regulatory practice applicable to the importer, document such assessment and provide it to the competent supervisory authority when asked to do so.
- The joint opinion 1/2021 of the EDPB and EDPS on the new SCCs clarifies that such an assessment should be based on objective factors and not the “the likelihood of a request in a specific case”. For transfers to the US, that means that the Foreign Intelligence Surveillance Act (FISA) and the US Executive Order 12333 and will actually make it impossible for the parties to simply sign the new SCCs without taking further steps to protect the data.

TIA_s

- TIAs (or TRAs in the UK): Conducting a TIA is a legal obligation for all EU-based data exporters who intend to carry out a restricted transfer by relying on one of the transfer tools in Article 46 of the GDPR.
- This assessment should be used always as a supplementary safeguarding.
 - First step is always a clear mapping of the data and data flows implemented
 - Second, to choose the right transfer vehicle (usually SCCs)
 - Third the analysis of the importer's jurisprudence
 - Fourth the European Essential Guarantees

TIAAs

➤ Analysis of the importer's jurisprudence

The operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data. Thus, Articles 7 and 8 of the Charter apply to this specific operation and their protection extend to the data transferred and data subjects must be afforded a level of protection essentially equivalent to that which is guaranteed within the European Union. The Charter includes a necessity and proportionality test to frame limitations to the rights it protects. According to the CJEU, the protection of the right to privacy requires that derogations from and restrictions to the right to data protection “must apply in so far as is strictly necessary”.

➤ The European Essential Guarantees

Following the analysis of the jurisprudence, the EDPB considers that the applicable legal requirements to make the limitations to the data protection and privacy rights recognised by the Charter justifiable can be summarised in four European Essential Guarantees:

- A. Processing should be based on clear, precise and accessible rules
- B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- C. An independent oversight mechanism should exist
- D. Effective remedies need to be available to the individual

What is the reality?

- International data transfers, especially towards the USA, have been a real issue the last 4 years. Especially since 2021, when CJEU issued the 'Schrems II' that invalidated the Privacy Shield adequacy system, companies were kept in a state of ambiguity on whether and under which conditions they could transfer any data outside the EU.
- Eventhough in 2021 the European Commission unraveled its renewed Standard Contractual Clauses (SCCs), to be adopted until December 2022 by the market and the EDPB adopted its final recommendations on "supplemental measures" still, not steady ground exists for international data transfers mainly due to the fact that the accountability principle implemented by the GDPR provides that each organization should make its own assessments whether the jurisdiction outside the EU provides for adequate data protection.

What is the reality?

- Adequacy is the best tool.
- The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.
- The UK and the US recently provided an update on UK-US data flows following the US C.L.O.U.D. Act that may hinder the UK's adequacy (another headache for EU controllers).

Updates

- On Oct. 7, after President's Joe Biden issued an "Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities", the Department of Justice supplemented it with a new regulation.
- As explained by the European Commission, this executive order establishes "a new two-layer redress mechanism, with independent and binding authority." In the first layer, "EU individuals will be able to lodge a complaint with the so-called 'Civil Liberties Protection Officer' of the US intelligence community." In the second layer, EU individuals would have the right to appeal that decision to the newly created Data Protection Review Court.
- The DPRC will have powers to investigate complaints from EU individuals, including to obtain relevant information from intelligence agencies, and will be able to take binding remedial decisions. For example, if the DPRC would find that data was collected in violation of the safeguards provided in the Executive Order, it will be able to order the deletion of the data.

How the DPO is implemented?

- The DPO should advise a controller or/and a processor on possible transfer issues
- The DPO should be implemented in the TIA and be aware that, the EDPB, as part of its recommendations, warns organizations transferring data not to rely on "subjective factors, such as the possibility of public authorities accessing the data in a way that is not in line with EU standards", but to look at the laws that govern access and level of protection, thus giving equal weight to both who has access to data and by what processes.
- If no adequate level of protection exists should advise for no data transfer
- The DPO should pay special attention when reviewing art 28 (Data Protection Agreements) so all transfer issues are addressed in an accountable and clear manner.