

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

GDPR Principles relating to processing of personal data

Dalibor Formánek

Milan, 17 April 2023



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

# Introduction

- Holubová advokáti s. r. o. (law firm), Czech Bar Association
- Located in Prague, Czech Republic and operates since 1991
- Travel law, personal injury, corporate, start-ups, real estate transactions, professional liability cases and **GDPR mainly for schools**

# What is GDPR?

- GDPR = comprehensive **data privacy regulation** that came into effect in the European Union on May 25, 2018
- Primary aims - **protect personal data** and provide data subjects (natural persons) with greater control over their personal information
- Directly binding and applicable – Regulation, not Directive
- Model for many other laws – Brazil, Argentina, Chile, California Consumer Privacy Act ...

# Principles

- Article 5
- Key rules for data controller and should lie at the heart of controller's approach to processing personal data
- Compliance with the “spirit“ of data protection regime
- GDPR is based on **7 key principles**:
  - 1. Lawfulness, Fairness and Transparency**
  - 2. Purpose Limitation**
  - 3. Data Minimization**
  - 4. Accuracy**
  - 5. Storage Limitation**
  - 6. Integrity and Confidentiality**
  - 7. Accountability**

# Lawfulness

- Personal data must be processed **lawfully**, that means the obligation to process data only in a way that is in **accordance with the law**, i.e. in accordance with the **GDPR and other legal regulations**
- Identify appropriate **lawful basis** under Art. 6 or exceptions stated in Art. 9 (condition for processing special categories) + don't do **anything generally unlawful** with personal data
- Reflected in Art. 6-10
- Example: The legal basis for processing does not have to be stated directly in the GDPR, it can also be based on the law of a Member State, but only where the GDPR provides for it, for example **Art. 85 + § 17 of Act. n. 110/2019 Coll.** regarding journalistic and similar purposes
- Example: **§ 28 of Czech Act. n. 561/2004 Coll.** states which data should be included in school evidence/register. If more data is included than it is stated in the domestic law, principle of lawfulness is breached.

# Fairness

- **Fairness** is the most general and vague of the principles and it applies to general fairness, or the fairness of processing data **above the legal framework**
- **Reasonable expectation** of data subjects
- Not to use data in the way that has **unjustified adverse effects** on data subjects
- Example: In practice it is the obligation of the controller to actively assist the data subject in exercising his or her rights, for example by providing additional information
- Example: arrangements between the controller and data subjects whereby the data subject should periodically check the data Privacy Policy published by the controller to ensure that it has not been amended or updated
- Example: collection of personal data for the purpose of imposing a fine for breaking the speed limit is justified and therefore not unfair

# Transparency

- The principle of **transparency** is closely related to the principle of **fairness** and requires that all information and all communications relating to the processing of personal data should be easily **accessible** and **understandable** and be presented using clear and plain language
- **Who? Why? How?** is somebody processing my data
- Reflected in Art. 13-14 (right to be informed)
- Example: Data subject should be informed about who is handling his/her data (controller) and why (purpose of processing). In practice, Czech supervisory authority places particular emphasis on the practical possibility for data subjects to contact and reach such a controller, i.e. on its accessibility and identifiability (inspection report UOOU-09488/14).

# Purpose Limitation

- Personal data must be collected **for specified, explicit and legitimate** purposes
- Data controller must be **clear about what** his purposes are from the start – why data are processed
- Record purposes in controller's **documentation and privacy information** for individuals
- It is possible to use data for **new purposes** if either this is **compatible** with the original purpose, you get **consent**, or there is a **clear obligation or function set out in law**
- Example: The headmaster makes the list of pupils available to his wife, who runs a travel agency, so that she can approach their parents with offers of language stays. Such processing is contrary to the original purpose for which the information was collected, namely the provision of education.

# Data Minimization

- Personal data collected must be **adequate, relevant, and limited** to what is necessary for the purposes for which it is processed. On the other hand, it is necessary to accept the processing of data **necessary to achieve** the **objective** pursued.
- Example: The processing of a name and surname in connection with a description of an event is not sufficient to identify the person and bring an action. For this purpose, it appears necessary to obtain also the address or identity number of that person (ECJ judgment of 4 May 2017, C-13/16, Rīgas satiksme)

# Accuracy

- Accuracy combines two requirements, the first is the requirement for the accuracy of the **data processed at the time they are obtained** and the second is the requirement to **update** them if changes occur **over time**.
- Rectify or delete inaccurate data
- Example: A healthcare provider must ensure that the medical records of their patients are accurate and updated regularly. If a patient informs the provider of an error, the provider must correct it.
- Example: In its judgment of 20 December 2017, C-434/16, Peter Nowak, the ECJ expressed the opinion that the accuracy and completeness of personal data must be assessed in the light of the purposes for which they were collected.

# Storage Limitation

- Personal data should be kept in a form that allows the identification of data subjects for **no longer than necessary** for the purposes for which the data is processed, the data is subsequently either **erased or anonymised**
- Example: A company should delete customer data when it's no longer needed for the purpose it was collected, such as after the termination of a service agreement or the completion of a project.
- The controller is obliged to determine in an **appropriate manner** the period of time for which the data will be processed/kept, this period should in principle be clear to the controller before the processing begins and it depends on the purpose
- The period of storage is **determined by the controller**, it isn't excluded, of course, that this period of storage might be determined directly by the **legislation** or that the legislation will determine the minimum or maximum period of storage

# Integrity and Confidentiality (security)

- Personal data must be processed in a manner that ensures **appropriate security**, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage
- Example: A bank must implement encryption, access controls, and other security measures to protect customer information from unauthorized access, data breaches, or other security threats
- A key approach to ensuring data security is a **risk-based approach**, that can then be used to determine the level of appropriate security, as part of that process, the controller or processor should assess the risks associated with the processing and take measures to mitigate risks **on their own**, these measures should ensure an appropriate level of security, including confidentiality, taking into account **the state of the art, the cost of implementing** the security measures **in relation to the risk** and the nature of personal data

# Accountability

- It incorporates genuine elements of **responsible data processing**, both in terms of compliance with the **legal text** and in terms of **treatment of data subjects** and **protection of their rights**
- **Responsibility for what the controller does with personal data and how he complies with other principles + he has to demonstrate the compliance**
- A big company **should have a data protection officer (DPO) responsible for ensuring GDPR compliance**, maintain records of data processing activities, conduct privacy impact assessments, and provide staff training on data protection
- This principle emphasizes the importance of safeguarding personal data, respecting user privacy, and ensuring transparency in data processing. Non-compliance with GDPR can result in **significant fines** and **reputational damage** for organizations

# Principles that are not explicitly stated in article 5

- Principle of proportionality
- Principle of subsidiarity
- Principle of restriction of transfer to a third country
- Principle of enhanced child protection
- Principle of protection of reasonable expectations
- Principle of a risk-based approach
- (Principles of procedural law)

# Sanctions

- Only breaches of the principles explicitly listed in Article 5(1) may be sanctioned, not any other principles that may apply to the processing of personal data
- Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the key principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to 20 000 000 EUR, or 4% of your total worldwide annual turnover, whichever is higher.
- Czech authority is not very strict

# Conclusion

- Reflect complex personal data legal framework
- Fundamental building block for a good data protection regime
- Key principles are both related and opposed
- They have their significance in interpretation and application of law
- Art. 5 – 6 – most sanctions

# Time for your questions

- [dalibor.formanek@holubova.cz](mailto:dalibor.formanek@holubova.cz)

Thank you!

Dalibor Formánek  
[info@holubova.cz](mailto:info@holubova.cz)

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

Data protection and justice legal framework

Federica Resta

Milan, 17 April 2023



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

# Data protection and justice

## Legal framework

In the relationship between data protection and justice is expressed, more than any other, the social function of privacy, indicated by R 4 as constitutive of this discipline because, precisely, it regulates a right that is never a tyrant, continually exposed to balancing with other legal interests as well as the ever-changing relationship with technology.

The GDPR provides that judicial protection, in civil and criminal cases, investigative needs and the same need to guarantee the independence of the judiciary constitute prerequisites for the limitation of the rights of the persons concerned (Article 23), and excludes the power of control of the data protection authorities for the requirements of due separation of powers and the guarantee of the independence and autonomy of the judiciary, also legitimising Member states to exclude judicial bodies from the obligation to designate the DPO (a faculty which Italy, for example, has not availed itself of).

The Italian rules has also excluded the applicability of administrative sanctions to the processing of personal data carried out by judicial authorities in the exercise of their judicial function and has specified that the procedural use of personal data is governed by the rules of procedural law. This is an important clarification, which renders consistent two disciplines (the data protection discipline and the procedural one) that are in any case both applicable to the processing of personal data in judicial proceedings and that must therefore be harmonised

On the contrary, the great innovation of the new European legal framework of 2018 consists precisely in its applicability also to the processing of personal data in judicial proceedings, both civil and criminal, with a modulation guaranteed above all by the prevalence of principles that are sufficiently broad and ductile to ensure the necessary coordination with the procedural discipline.

The principles of minimisation and lawfulness, for instance, could well be valorised with respect to the complex issue of the admissibility of so-called unlawful evidence, i.e. evidence obtained by incisively violating the subject's privacy. If, in fact, in the Italian criminal trial there is a rule of evidentiary exclusion of evidence that has been unlawfully formed and in any case is such as to violate the dignity of the person, in the Italian civil trial (inspired by the dispositive, not acquisitive, principle) there is no such rule

The principles of data protection may well be assessed on this basis too, balancing data protection and evidential necessity.

A useful tool may also be, for instance, the obscuring of surplus data also with the help of the judge, so as to exercise the powers of direction of the trial referred to in Article 175 of the Code of Civil Procedure, which are precisely aimed at the "fair conduct of the trial".

An undoubtedly well-balanced discipline was clearly dictated by the previous national rules where the confidential information concerned a person's sex life or health. In this case, Article 26(4)(c) provided that personal data could only be used in legal proceedings, even in the absence of the data subject's consent, on condition that the right asserted by the data subject was of 'equal rank' to that of the supersensitive data controller. This provision has now been deleted but is indirectly derived from Art. 6(1)(f) of EU Reg. No. 679/2016 on balancing criteria.

It must, however, be borne in mind that the right to be balanced with the right to privacy is not the right of action or defence (on pain of an emptying of the rule), which is always per se of constitutional rank, but the substantive right that is the subject of the request for protection in court.

Even more significant, then, are the derogations and specificities imposed, in the field of criminal justice, by Directive 2016/680. The regulation of processing operations in the courts has been brought within the general legislation (albeit with the necessary modulations), with the exception of criminal justice, the specificities of which have instead imposed differentiated rules, in accordance with the indications of Declaration 21 annexed to the Lisbon Treaty

Naturally, the regulation of the processing of personal data in the judicial context involves not only the judicial bodies but also the defence, the lawyers, those who, that is, must guarantee judicial protection in the most effective way also, of course, by collecting and supplying personal data in court, including data deserving of enhanced protection such as special data. Data protection requirements are, moreover, complementary to the guarantees of professional secrecy, strengthening them and making them more effective

An important instrument of guarantee are, in the Italian legal system, also the deontological rules: true regulatory sources with reserved competence, which supplement the rule of law by introducing specific and additional obligations, common to the professional category of reference, to ensure greater effectiveness of the discipline. The deontological rules for lawyers are, in this sense, particularly relevant, also because they provide clear indications that are modulated on the specific reality of reference

Useful measures are envisaged for the performance of defensive investigations, as such liable to entail even invasive processing of personal data and therefore deserving of special precautions. Also important are the rules of confidentiality prescribed in relations with the press, always inspired by the protection of the assisted person. Also important are the measures for the storage of data and their deletion as soon as the defence needs cease to exist and the rules to be observed in relations with other professionals and with the Bar Council itself.

These are rules applicable to the entire management of the relationship with the client and third parties, irrespective of the distinction between the civil and criminal sectors. In the latter area, then, the lawyer is confronted with one of the most significant (but, paradoxically, also least known) components of the new European data protection legal framework, that is Directive 2016/680 (LED).

The Directive lays down rules - mirroring those of the General Data Protection Regulation (GDPR) 2016/679 - on the protection of personal data in the exercise of police and criminal justice activities, but entrusting it to a legal instrument for the harmonisation (and not the direct unification) of legislation, due to the peculiarities of the matter and the diversity of procedural systems between Member States.

Directive 680 therefore constitutes an express limitation to the objective scope of the Regulation, pursuant to Article 2(2)(d) of the GDPR, relating precisely to the processing of personal data for the purpose of 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-

.

The exclusion does not only concern the area of criminal and police cooperation, which is the subject of Declaration 21 annexed to the Final act of the Intergovernmental Conference which adopted the Treaty of Lisbon (Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation) . The real novelty of the Directive 680 (especially with respect to the Framework Decision 2008/977 of the Council which it repeals) concerns, in fact, the applicability of its rules not only to the cooperative sphere, but also to the (criminal) judicial and police activities in the internal sphere

The distinction of the scope of application between the Regulation and Directive 680 is, therefore, entirely based on the twofold subjective element (carrying out of the processing by national authorities competent in the matters identified) and teleological-functional element (pursuit of the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the protection against and prevention of threats to public security).

The final text outlines an appreciable balance between investigative needs and data protection, represented, for example, by the general principles to which the processing must conform, in any case (based, in particular, on the principles of fairness, lawfulness and functionality of the processing with respect to the institutional purposes pursued).

. Also important are the rights acknowledged to the data subject (among which also that to the limitation of the processing), even if compressible - besides where provided for by the criminal procedural law - also, albeit in a proportional measure, by reason of particular investigative or security needs, provided that the limitation "constitutes a necessary and proportionate measure in a democratic society, with due regard to the fundamental rights and legitimate interests" of the data subject, according to the definition of the ECHR).

**Legislative decree n. 51/18** provides in particular, as essential choices:  
definition of competent authorities in accordance with the wording of the Directive;

mandatory appointment of the Data Protection Officer also for the judicial authority in the exercise of its functions (whereas the Directive also allowed this to be waived);

referral to a specific Presidential Decree (not yet issued) for the detailed provision of individual processing operations, with the precise regulation of storage periods, access procedures, etc., administrative sanctioning cases modulated (as to conduct and application criteria) on those of the regulation .....

.....strong protection (also of third parties) involved in criminal proceedings against the processing of their data contained in judicial documents;

limitation of the exercise of the rights of the data subject (without a 'reasoned notice' to the data subject being required in any case) if this would compromise the investigation or for reasons relating to the protection of public security, national security or the rights and freedoms of others;

identification of the Garante as the single national supervisory authority, except for processing carried out by the judicial authority in the exercise of its judicial functions, as well as the judicial functions of the public prosecutor.

No other authority was indicated for these processings, but the control of legitimacy was referred to the same court, with the instruments of the trial, according to the solution adopted by the German legislator.

Legislative Decree 51 of 2018 brings some important innovations.

In the first place, the introduction, in Art. 14, of the right of "whoever has an interest (therefore, also of the third party) to request the rectification, cancellation or limitation of his data contained in judicial acts or investigations, also in the trial, with the modalities provided for by Art. 116 code of criminal procedure (this rule is particularly important also for the purposes of the data intercepted during interception, as we shall see below).

Secondly, it is important to note the introduction of a specific criminal offence modelled on the unlawful processing of personal data (with intent to cause damage or profit and an objective condition of liability based on the harm caused to the person concerned) aimed at punishing the forms of abuse of the processing power to the detriment of the citizen, carried out in violation of certain particularly relevant rules (those on automated decisions, those on the conditions of processing of particular data, and those on the general conditions of lawfulness of the processing).

One of the most important innovations introduced by the internal legislator concerns, however, the provision, in Art. 14, of the right of "anyone who has an interest in it" (therefore, also of the third party) to "request the rectification, deletion or limitation of his data contained in judicial acts or investigations, also in trial, with the modalities provided for in Art. 116 c.c.p.", specifying that "the Judge provides for it in the forms of Art. 130 of the Code of Criminal Procedure.

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

Data controller and data processor

Filippo Bianchini

Milan, 17 April 2023



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

>\_who I am

Training of Lawyers on  
EU Law relating to Data  
Protection 2

- Barrister, qualified to the Higher Courts
- Member of the CNF Privacy Commission and of the FIIF Working Group
- UNI 11697:2017 certified DPO and Privacy Evaluator – ISO 27001:2013 Lead Auditor – CIPP/E
- Lecturer at the Master in "Data protection, cybersecurity and digital forensics" at University of Perugia
- Advanced training in "Legal tech", "Data Governance & Data Protection" and "Cybercrime and digital investigations" at University of Milan



#TRADATA2

# What we will talk about

Training of Lawyers on  
EU Law relating to Data  
Protection 2

## Privacy roles

- The controller
- The processor
- The joint controller

## Obligations and liability

- Regulatory obligations
- Responsibilities and their allocation

## The agreements

- Data communication agreement
- Data processing agreement



#TRADATA2

ARTICLE 29 DATA PROTECTION WORKING PARTY



00264/10/EN  
WP 169

Opinion 1/2010 on the concepts of "controller" and "processor"

Adopted on 16 February 2010

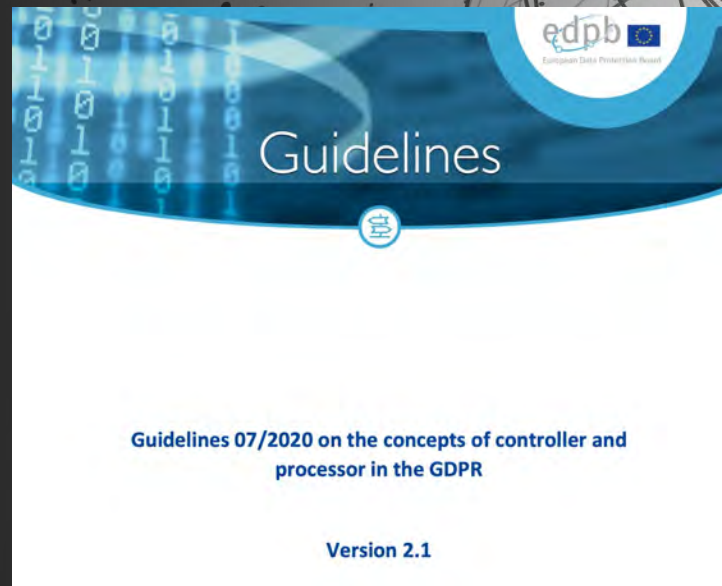
Training of Lawyers on  
EU Law relating to Data  
Protection 2




#TRADATA2

# Privacy roles

---





Training of Lawyers on  
EU Law relating to Data  
Protection 2

 #TRADATA2

Data controller

---

# The data controller

Training of Lawyers on  
EU Law relating to Data  
Protection 2

Definition

Purposes of the processing

Means of the processing

- **Essential** means
- **Non-essential** means

Responsibility of the organisation  
as a whole

Ownership irrespective of contact  
with the data



#TRADATA2

# The data controller

Training of Lawyers on  
EU Law relating to Data  
Protection 2




#TRADATA2

## Identifying the data controller

1. Direct relationship with stakeholders
  - Employers and insurance companies
  - Payment service providers
2. Legal obligation
  - Airline reservation systems
3. Benefits and distinct purposes deriving from the processing

## Autonomous Ownership

- Transfer of marketing database
- Transfer of a branch of business



Training of Lawyers on  
EU Law relating to Data  
Protection 2

 #TRADATA2

Data processor

---

# The data processor

Training of Lawyers on  
EU Law relating to Data  
Protection 2

Definition

Processor vs. appointee

Companies providing payroll services

"Irrelevant" processing

- Taxis and delivery
- Maintenance and cleaning

Controller's instructions

Excesses



#TRADATA2

# The data processor

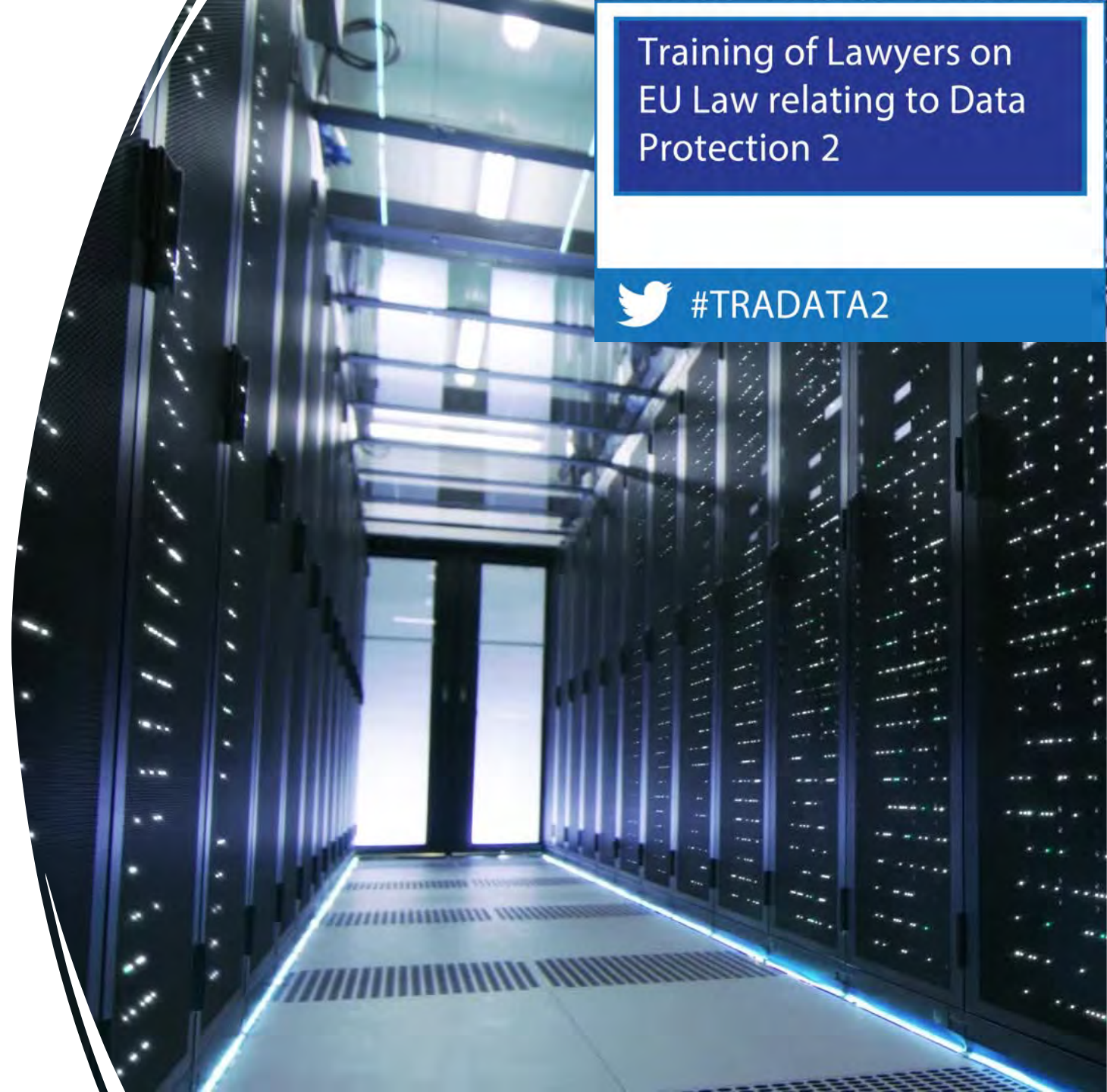
---


- Grey areas
  - Owners or managers?
  - Relationships between customers and suppliers (B2B)
  - Cloud Providers
  - Intermediaries (e.g. head-hunters, agencies)

Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2





Training of Lawyers on  
EU Law relating to Data  
Protection 2

 #TRADATA2

Joint controller

---

# The data processor

Training of Lawyers on  
EU Law relating to Data  
Protection 2



Definition



Shared Purposes and Means



Online advertising

Facebook fan pages and  
use of Insight services  
Fashion ID Case



[The EDPB Guidelines on Social Media Targeting](#)

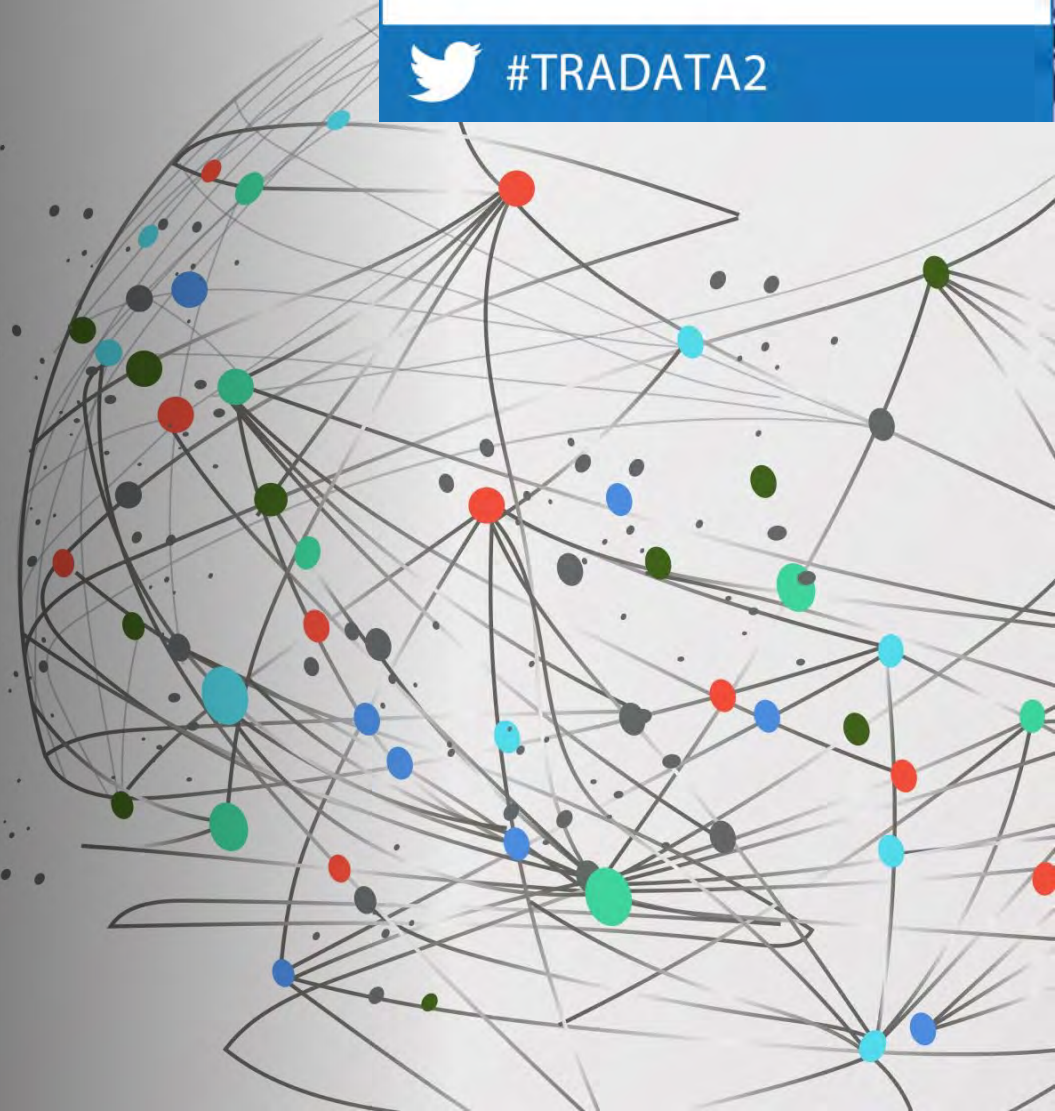



#TRADATA2



# Obligations and liability

---





Training of Lawyers on  
EU Law relating to Data  
Protection 2

 #TRADATA2

# Regulatory obligations

---

Regulatory  
obligations


Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2

Obligations of the  
data controller

Obligations of the  
data processor



Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2



# Responsibilities and their allocation

---

# Responsibilities and their allocation

Training of Lawyers on  
EU Law relating to Data  
Protection 2

Joint and several liability  
(Art. 82)

Responsibilities of the  
sub-processor (Art.  
28(4))

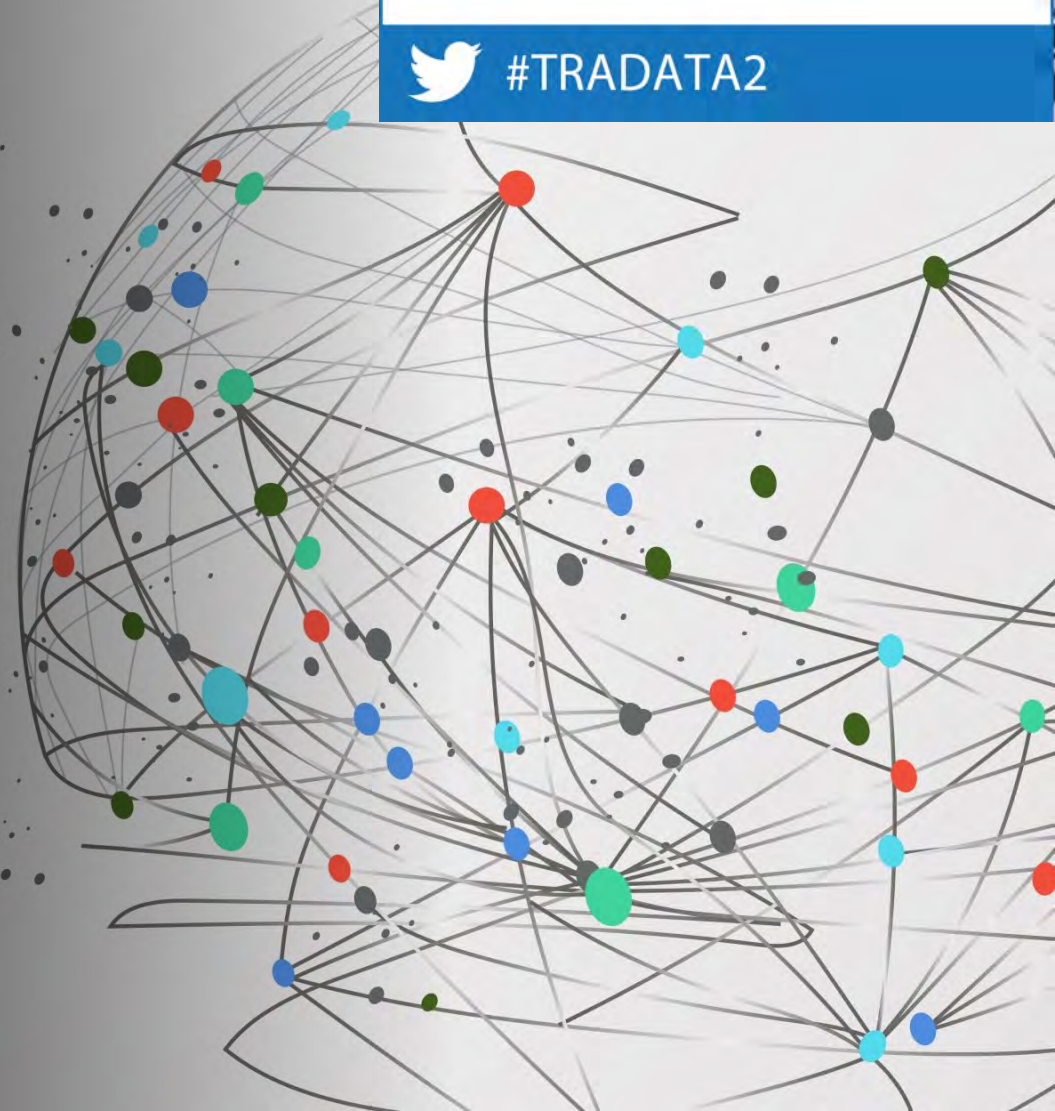


#TRADATA2



# The agreements

---





# Data Communication Agreements

---

Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2



# Data Processing Agreement

---

Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2

# Data Processing Agreements (DPA)

Training of Lawyers on  
EU Law relating to Data  
Protection 2

## Preliminary verification

- Due diligence

## Written authorisation

## Minimum statutory content

- Details on the scope of processing
- The obligations of the processor

## Negotiating autonomy



#TRADATA2

Future  
challenges

Training of Lawyers on  
EU Law relating to Data  
Protection 2

Blockchain

Web3



#TRADATA2

Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2

Thank you  
for your attention!

---

Filippo Bianchini

Phone: (+39) 349 2864103 – E-mail: [info@bianchini.legal](mailto:info@bianchini.legal)

LinkedIn: [studiolegale](https://www.linkedin.com/company/studiolegale) – Twitter: [@legale](https://twitter.com/@legale)

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

Rights of the data subject, including criminal  
investigations and proceedings

Giovanni Battista Gallus

Milan, 17 April 2023



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

# IL PROCESSO DI ADEGUAMENTO AL GDPR

SECONDA EDIZIONE

A cura di  
Giuseppe Cassano, Vincenzo Colarocco,  
Giovanni Battista Gallus, Francesco Paolo Micozzi

Prefazione di  
Ginevra Cerrina Feroni

M. Barbarossa, U. Bardari, C. Benvenuto, E. Casadio, V. Cerocchi,  
V. Colarocco, A. d'Agostino, I. Destri, F. Faini, G.B. Gallus, T. Grotto,  
M. Iaselli, A.M. Lotto, G. Marino, F.P. Micozzi  
M. Pintus, R. Quintavalle, L. Scudiero, S. Stefanelli

**GIUFFRÈ**  
GIUFFRÈ FRANCIS LEXISNIE



## Who am I

- Lawyer - [array.eu](http://array.eu)
- Master of Laws in Maritime Law and Information Technology Law - University College London
- Working group member – Italian Foundation legal Innovation (FIIF)
- Member of Surveillance Commission - CCBE (Council of Bars and Law Societies of Europe)
- Fellow of NEXA Center – Polytechnic of Turin
- Advisory Board Member – Drone Observatory on Drones and Advanced Air Mobility – Polytechnic of Milan
- Data protection officer



# Main topics

---

- Data subject rights (DSR) – introduction
- Common principles
- DSR & accountability
- A quick overview of the rights
- Focus on the right of access
- DSR and law enforcement directive
- DSR in the context of the European Data Strategy and the Digital services package

## Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2



Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)

Adopted on 29 November 2017



**Guidelines 3/2019 on processing of personal data through video devices**

Version 2.0  
Adopted on 29 January 2020



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

Adopted on 29 November 2017  
As last Revised and Adopted on 11 April 2018



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

Version 1.0  
Adopted on 18 January 2022



**Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)**

Version 2.0  
Adopted on 7 July 2020



Guidelines on the right to data portability

Adopted on 13 December 2016  
As last Revised and adopted on 5 April 2017

# Useful guidelines

Training of Lawyers on  
EU Law relating to Data  
Protection 2

HANDBOOK



Handbook on European  
data protection law

2018 edition



#TRADATA2

# Common principles

# Data Subject rights - definitions

We all know the  
definition of  
Personal data...

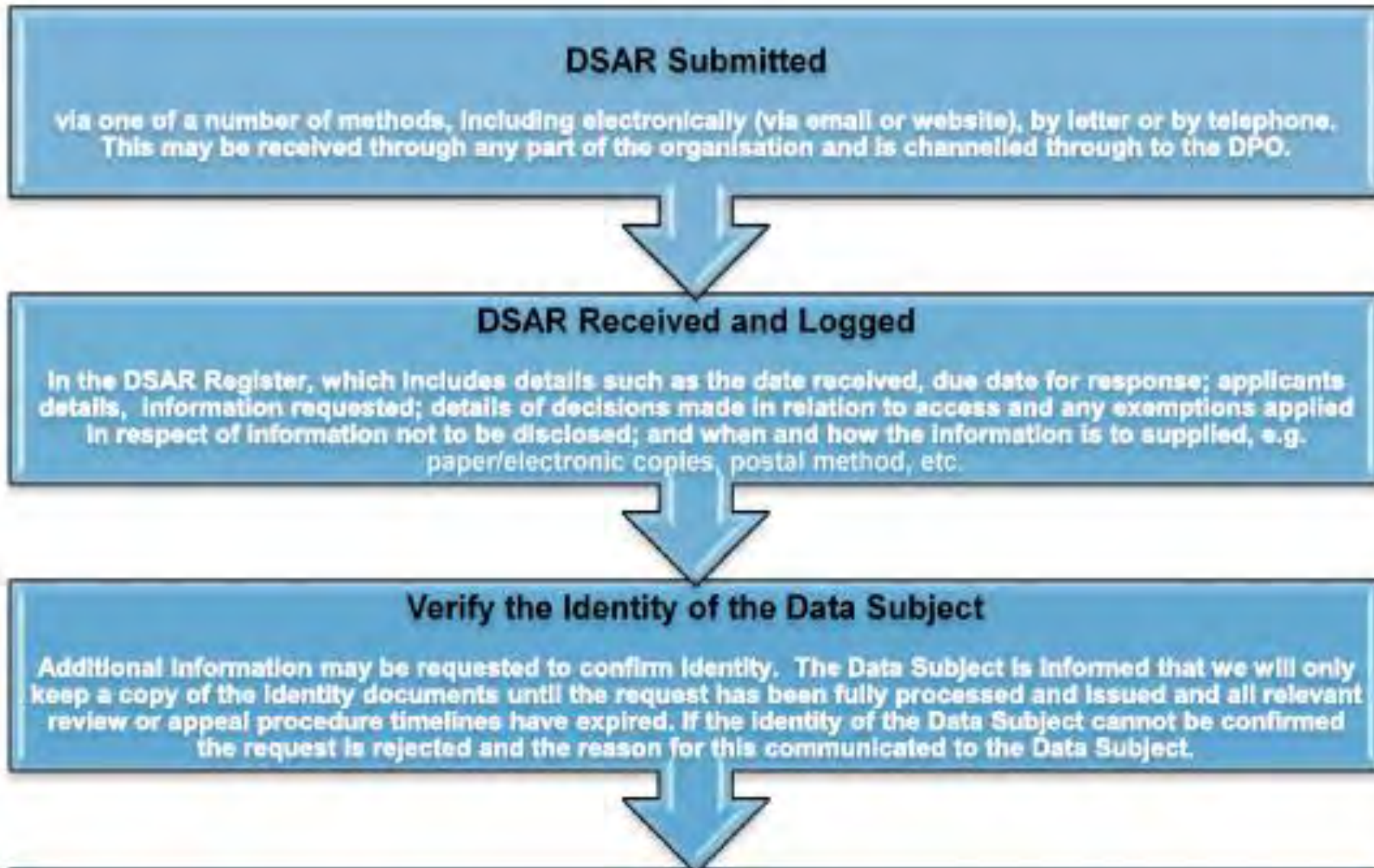


We all know  
who the Data  
subject is...

Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2



# Identification?

- Need for identification
- if the controller has doubts about whether the data subject is who they claim to be, the controller must request additional information in order to confirm the identity of the data subject. The request for additional information must be proportionate to the type of data processed, the damage that could occur etc. in order to avoid excessive data collection.



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

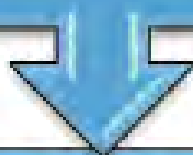
**Version 1.0**

**Adopted on 18 January 2022**



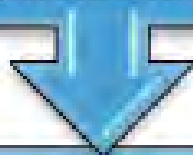
### Evaluate Validity of Information Provided

If necessary, steps are taken to check the accuracy of the information provided by the Data Subject.



### Identify and Compile the Personal Data

Data flow diagrams and data inventories are used to pinpoint the systems that store the requested personal data (if applicable). Staff are emailed to request any information that may be within their area regarding the request. The personal data is compiled.



### Respond to Data Subject

The Data Subject is provided with a response and copies of any personal data capable of being provided.



### Close DSAR

The fact that the request has been responded to is logged in the DSAR Register together with the date of closure.

# Time limit to respond (art. 12)

As soon as possible - one month maximum

It can be extended by two further months where necessary, taking into account the complexity and number of the request

The data subject has to be informed about the reason for the delay

# Formalities for the answer (art. 12)

Concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

In writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally

# Importance of Legal Design

- Legal design is the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying (M. Hagan)



In this introductory chapter, I introduce the concept of 'Legal Design' & define what Design and Design Thinking mean.

## What is Legal Design?

Legal design is the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying.



# Can the request be refused (art. 12)?

- Yes, when it is manifestly unfounded or excessive;
- In such cases, a reasonable fee for such requests can be applied instead of the refusal
- These concepts have to be interpreted narrowly
- Burden of proof rests on the controller
- Restrictions may also exist in Member States' national law as (Art. 23 GDPR)



# Video surveillance

- Given that any number of data subjects may be recorded in the same sequence of video surveillance a screening would then cause additional processing of personal data of other data subjects. If the data subject wishes to receive a copy of the material (article 15 (3)), this could adversely affect the rights and freedoms of other data subject in the material.
- If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject.
- Guidelines 3/2019



# The duty to answer (according to the Italian Supreme Court – decision 9313/2023 – 4/4/2023)

- “With regard to the processing of personal data, the subject of the obligation to provide an answer regarding the possession (or not) of the sensitive data is the recipient of the access request and not the applicant, the first having to always answer the request of the data subject, even in negative terms, expressly declaring that he is, or not, in possession of the data of which it is required the ostension”

Numero registro generale 8263/2021

Numero sezionale 1073/2023

Numero di raccolta generale 9313/2023

Data pubblicazione 04/04/2023



**REPUBBLICA ITALIANA**  
**LA CORTE SUPREMA DI CASSAZIONE**  
**PRIMA SEZIONE CIVILE**

Composta dagli Ill.mi Sigg.ri Magistrati

Oggetto

Dott. Francesco <small>(omissis)</small> Genovese	Presidente
Dott. Laura Tricomi	Consigliere
Dott. Giulia Iofrida	Consigliere
Dott. Loredana Nazzicone	Consigliere
Dott. Roberto Amatore	Consigliere - Rel.

PROTEZIONE DATI  
PERSONALI

Ud. 24/2/2023 CC

ha pronunciato la seguente

**ORDINANZA**

sul ricorso n. 8263-2021 r.g. proposto da:

# A quick overview of the rights

A quick  
summary of DSR  
(from the  
Handbook on  
European data  
protection law)

EU	Issues covered	CoE
<b>Right to be informed</b>		
General Data Protection Regulation, Article 12  CJEU, C-473/12, <i>Institut professionnel des agents immobiliers (IPI) v. Englebert</i> , 2013  CJEU, C-201/14, <i>Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others</i> , 2015	Transparency of information	Modernised Convention 108, Article 8
General Data Protection Regulation, Article 13 (1) and (2) and Article 14 (1) and (2)	Content of information	Modernised Convention 108, Article 8 (1)
General Data Protection Regulation, Article 13 (1) and Article 14 (3)	Time of providing information	Modernised Convention 108, Article 9 (1) (b).
General Data Protection Regulation, Article 12 (1), (5) and (7)	Means of providing information	Modernised Convention 108, Article 9 (1) (b).
General Data Protection Regulation, Article 13 (2) (d) and Article 14 (2) (e), Articles 77, 78 and 79	Right to lodge a complaint	Modernised Convention 108, Article 9 (1) (f)

A quick  
summary of DSR  
(from the  
Handbook on  
European data  
protection law)

<b>Right of access</b>		
<b>EU</b>	<b>Issues covered</b>	<b>CoE</b>
General Data Protection Regulation, Article 15 (1) CJEU, C-553/07, <i>College van            burgemeester en wethouders van</i>	Right of access to one's own data	Modernised Convention 108, Article 9 (1) (b) ECtHR, <i>Leander</i>
CJEU, Joined cases C-141/12 and C-372/12, <i>YS v. Minister voor            Immigratie, Integratie en Asiel and            Minister voor Immigratie, Integratie            en Asiel v. M and S</i> , 2014 CJEU, C-434/16, <i>Peter Nowak v. Data            Protection Commissioner</i> , 2017		
<b>Right to rectification</b>		
General Data Protection Regulation, Article 16	Rectification of inaccurate personal data	Modernised Convention 108, Article 9 (1) (e) ECtHR, <i>Cemalettin            Canli v. Turkey</i> , No. 22427/04, 2008 ECtHR, <i>Ciubotaru v.            Moldova</i> , No. 27138/04, 2010

A quick  
summary of DSR  
(from the  
Handbook on  
European data  
protection law)

### Right to rectification

General Data Protection Regulation,  
Article 16

Rectification  
of inaccurate  
personal data

Modernised  
Convention 108,  
Article 9 (1) (e)  
ECtHR, *Cemalettin  
Canli v. Turkey*,  
No. 22427/04, 2008  
ECtHR, *Ciubotaru v.  
Moldova*, No. 27138/04,  
2010

### Right to erasure

General Data Protection Regulation,  
Article 17 (1)

The erasure of  
personal data

Modernised  
Convention 108,  
Article 9 (1) (e)  
ECtHR, *Segerstedt-  
Wiberg and Others v.  
Sweden*, No. 62332/00,  
2006

CJEU, C-131/12, *Google Spain SL,  
Google Inc. v. Agencia Española de  
Protección de Datos (AEPD), Mario  
Costeja González* [GC], 2014

CJEU, C-398/15, *Camera di Commercio,  
Industria, Artigianato e Agricoltura di  
Lecce v. Salvatore Manni*, 2017

The right to be  
forgotten

A quick  
summary of DSR  
(from the  
Handbook on  
European data  
protection law)

<b>Right to restriction of processing</b>		
General Data Protection Regulation, Article 18 (1)	Right to restrict use of personal data	
General Data Protection Regulation, Article 19	Notification obligation	
<b>Right to data portability</b>		
General Data Protection Regulation, Article 20	Right to data portability	
<b>Right to object</b>		
General Data Protection Regulation, Article 21 (1) CJEU, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni</i> , 2017	Right to object due to the data subject's particular situation	Profiling Recommendation, Article 5.3 Modernised Convention 108, Article 9 (1) (d)

A quick  
summary of DSR  
(from the  
Handbook on  
European data  
protection law)

EU	Issues covered	CoE
General Data Protection Regulation, Article 21 (2)	Right to object to use of data for marketing purposes	Direct Marketing Recommendation, Article 4.1
General Data Protection Regulation, Article 21 (5)	Right to object by automated means	
<b>Rights related to automated decision-making and profiling</b>		
General Data Protection Regulation, Article 22	Rights related to automated decision-making and profiling	Modernised Convention 108, Article 9 (1) (a)
General Data Protection Regulation, Article 21	Rights to object automated decision-making	
General Data Protection Regulation, Article 13 (2) (f)	Rights to a meaningful explanation	Modernised Convention 108, Article 9 (1) (c)



# Let's not forget data breaches

- Right to be informed in the event of a data breach, if the breach is likely to result in a high risk to the rights and freedoms of natural persons



# DSR & accountability

# DSR & accountability

- A question:
- What are the accountability measures to be taken for compliance with DSRs?



# DSR and accountability

ICT systems able to respond quickly to DSRs (access, portability, erasure etc...) – art. 25

The screenshot shows a Microsoft Ignite event page. At the top left, it says "Microsoft Ignite" with the dates "October 12-14, 2022" and a "Register now" button. Below this is a navigation bar with "Microsoft", "Learn", "Documentation", "Training", "Certifications", "Q&A", "Code Samples", "Shows", and "Events". A search bar and "Sign in" link are on the right. A left sidebar contains a "Filter by title" search box and a list of categories: "Microsoft compliance offerings", "General Data Protection Regulation (GDPR)", "Accountability readiness checklists", and "Data subject requests". The "Data subject requests" category is expanded, showing sub-items like "Data subject requests", "Manage data subject requests with the DSR case tool", "Azure", "Azure DevOps services", "Dynamics 365", "Intune", "Microsoft Support & Professional Services", and "Office 365". The main content area features the article title "Office 365 Data Subject Requests for the GDPR and CCPA" with a breadcrumb "Learn / General Data Protection Regulation (GDPR) / Data subject requests /". Below the title is the article metadata: "Article • 09/27/2022 • 130 minutes to read • 5 contributors". The article content begins with "Introduction to DSRs" and a paragraph: "The European Union [General Data Protection Regulation \(GDPR\)](#) gives rights to people (known in the regulation as *data subjects*) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the *data controller* or just *controller*). Personal data is defined broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a *Data Subject Request* or DSR. The controller is obligated to promptly consider each DSR and provide a substantive response either by taking the requested action or by providing an explanation for why the DSR can't be accommodated by the controller. A controller should consult with its own legal or compliance advisors regarding the proper disposition of any given DSR." On the right side of the article, there is an "In this article" section with links: "Introduction to DSRs", "Part 1: Responding to DSRs for Customer Data", "Using the Content Search eDiscovery tool to respond to DSRs", and "Providing a copy of personal data". A "Show more" link is at the bottom of this section.

Adequate DSR policies (art. 24)

# DSR and accountability

**Data Subject Rights Policy**  
**Operational Guide for Personnel**  
**The Adoption Authority of Ireland**



ÚDARÁS UCHTÁLA na hÉIREANN  
THE ADOPTION AUTHORITY of IRELAND

Revision and Approval History					
Version	Revised By	Revision Date	Approved By	Approval Date	Comments
Draft	DPO	9/4/2019			
Reviewed	DPO	22/01/2020			
Reviewed	Matheson	19/10/2020			
Reviewed	DPO	28/01/2021			
Reviewed	DPO	1/04/2021			
Approved	Board	April 2021			



# DSR and accountability

- Regulation of DSR requests in Data protection agreements (art. 28) & joint controller agreements (art. 26)
- Instructions and training for any person acting under the authority of the controller or of the processor who processes personal data
- ...

Focus on the right of  
access

# The right of access

---

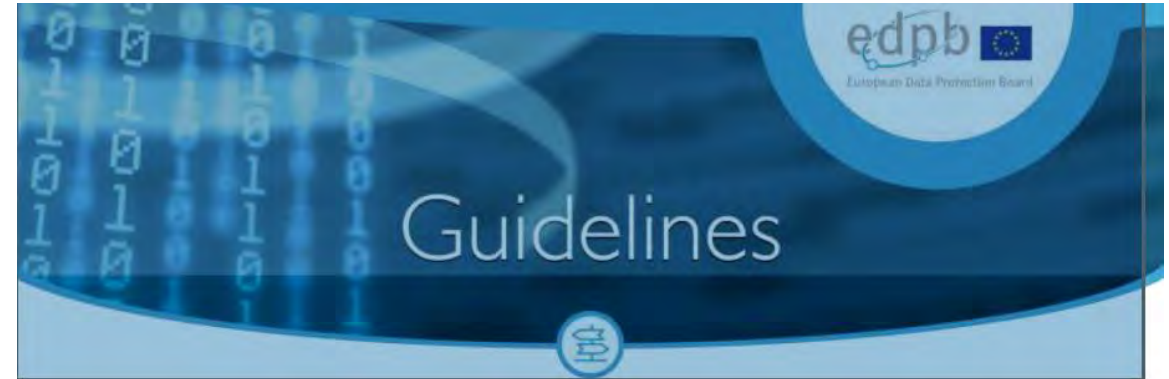
enshrined in Art. 8 of the EU Charter of Fundamental Rights.

---

Part of the European data protection legal framework since its beginning

---

Further developed by more specified and precise rules in Art. 15 GDPR.



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

**Version 1.0**

**Adopted on 18 January 2022**

# The right of access under the GDPR vs other access rights

**Access to  
public  
documentation**

**FOIA requests**

## Does the request need a specific format?



- Controller must provide appropriate and user-friendly channels
- the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller
- No need for motivation

## Employees' right of access: Italian SA fines Unicredit S.p.A. and orders corrective measures

 20 September 2022 Italy

### Background information


- > Date of final decision: 16 June 2022
- > Controller: Unicredit S.p.A
- > Legal Reference: transparency and fairness of processing (Article 5.1(a)), transparency in and arrangements for exercise of DSR (Art.12), right of access (Art.15)
- > Decision: the Italian SA imposed an EUR 70,000 administrative fine and ordered the controller to grant the access request by the data subject
- > Key words: processing of data in the employment sector, right of access to one's personal data, transparency and fairness of processing




### Summary of the Decision

#### Latest news

[Third fine imposed by Polish SA on the Surveyor General of Poland for failure to notify the personal data breach](#)

 23 September 2022 Poland

[Employees' right of access: Italian SA fines Unicredit S.p.A. and orders corrective measures](#)

 20 September 2022 Italy

[September plenary - adopted documents](#)

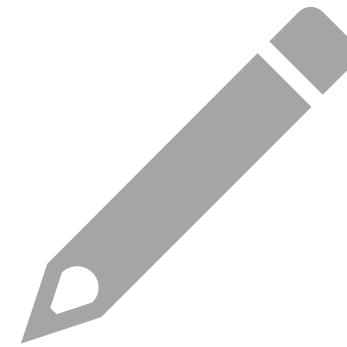
 20 September 2022 EDPB

[New EDPB opinion on certification criteria](#)

# The right of access – overall aim



Provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data.



Will facilitate the exercise of other rights such as the right to erasure or rectification.

# The right of access

---

three different components:

**Confirmation** as to whether data about the person is processed or not,

**Access to this personal data** and

**Access to information about the processing**, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers



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

**Version 1.0**

**Adopted on 18 January 2022**



[Pagina iniziale](#) > [Formulario di ricerca](#) > [Elenco dei risultati](#) > Documenti

Lingua del documento :  ECLI:EU:C:2023:3

Avvia la stampa

Provisional text

JUDGMENT OF THE COURT (First Chamber)

12 January 2023 (\*)

(Reference for a preliminary ruling - Protection of natural persons with regard to the processing of personal data - Regulation (EU) 2016/679 - Article 15(1)(c) - Data subject's right of access to his or her data - Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed - Restrictions)

In Case C-154/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 18 February 2021, received at the Court on 9 March 2021, in the proceedings

RW

Does the data subject have the right to know the specific identity of the recipients?  
ECJ, case [154/21](#)

- By its question, the referring court asks, in essence, whether Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject's right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the specific identity of those recipients.
- Recital 63 of that regulation states that the data subject is to have the right to know and obtain communication in particular with regard to the recipients of the personal data and does not state that that right may be restricted solely to categories of recipients
- Data controllers must comply with the principle of transparency
- Article 15 of the GDPR lays down a genuine right of access for the data subject, with the result that the **data subject must have the option of obtaining either information about the specific recipients to whom the data have been or will be disclosed, where possible, or information about the categories of recipient.**
- **The right of access is necessary to enable the data subjects to exercise the other rights (erasure, rectification etc.)**



Provisional text

JUDGMENT OF THE COURT (First Chamber)

12 January 2023 (\*)

(Reference for a preliminary ruling - Protection of natural persons with regard to the processing of personal data - Regulation (EU) 2016/679 - Article 15(1)(c) - Data subject's right of access to his or her data - Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed - Restrictions)

In Case C-154/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 18 February 2021, received at the Court on 9 March 2021, in the proceedings

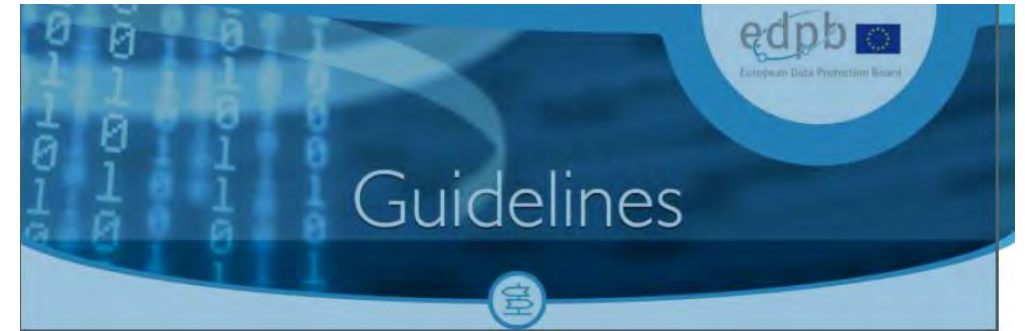
RW

Does the data subject have the right to know the specific identity of the recipients?  
ECJ, case [154/21](#)

- Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject's right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, **an obligation on the part of the controller to provide the data subject with the actual identity of those recipients**, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of the GDPR, in which cases the controller may indicate to the data subject only the categories of recipient in question.

# Access to information about the processing vs transparency obligations of art. 13-14 GDPR

- Any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the « tailored » information is the same as the « general » information.



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

**Version 1.0**

**Adopted on 18 January 2022**

# Which data?

- Unless explicitly stated otherwise, the request should be understood as referring to **all personal data concerning the data subject** and the controller may ask the data subject to specify the request if they process a large amount of data
- The communication of data and other information about the processing must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Layered approach



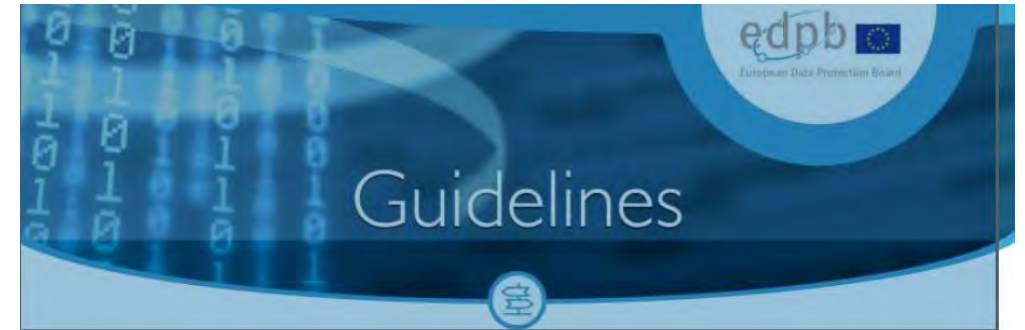
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

# Does it include inferred data?

- Data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment or a personalization or recommendation process)
- the right of access includes both inferred and derived data, including personal data created by a service provider, whereas the right to data portability only includes data provided by the data subject.
- Therefore, in case of an access request and unlike a data portability request, the data subject should be provided not only with personal data provided to the controller to make a subsequent analysis or assessment about these data but also with the result of any such subsequent analysis or assessment.



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

**Version 1.0**

**Adopted on 18 January 2022**

Case C-487/21

F.F.  
interested parties:  
Österreichische Datenschutzbehörde,  
CRIF GmbH

(Request for a preliminary ruling lodged by the Bundesverwaltungsgericht (Federal Administrative Court, Austria))

preliminary ruling - Protection of personal data - Regulation (EU) 2016/679 - Article 15(3) - Right of access by the data subject to personal data undergoing processing - Right to receive a copy of personal data - (Concept of 'information')

Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2

The exact boundaries  
of the right to obtain  
a copy according to  
the Advocate general  
(Case [C-487/21](#))

- the concept of 'copy' referred to in that provision must be understood as a **faithful reproduction in intelligible form of the personal data requested by the data subject, in material and permanent form, that enables the data subject effectively to exercise his or her right of access to his or her personal data in full knowledge of all his or her personal data that undergo processing** – including any further data that might be generated as a result of the processing, if those also undergo processing – in order to be able to verify their accuracy and to enable him or her to satisfy himself or herself as to the fairness and lawfulness of the processing so as to be able, where appropriate, to exercise further rights conferred on him or her by the GDPR; the exact form of the copy is determined by the specific circumstances of each case and, in particular, the type of personal data in respect of which access is requested and the needs of the data subject;
- that provision **does not confer on the data subject a general right to obtain a partial or full copy of the document that contains his or her personal data** or, if the personal data are processed in a database, an extract from that database;
- that provision does not rule out, however, the data subject having to be provided with portions of documents, or entire documents or extracts from databases, if that were necessary to ensure that the personal data undergoing processing and in respect of which access is requested are fully intelligible.

Case C-487/21

F.F.  
interested parties:  
Österreichische Datenschutzbehörde,  
CRIF GmbH

(Request for a preliminary ruling lodged by the Bundesverwaltungsgericht (Federal Administrative Court, Austria))

preliminary ruling - Protection of personal data - Regulation (EU) 2016/679 - Article 15(3) - Right of access by the data subject to personal data undergoing processing - Right to receive a copy of personal data - (Concept of 'information')

Training of Lawyers on  
EU Law relating to Data  
Protection 2



#TRADATA2

The exact boundaries  
of the right to obtain  
a copy according to  
the Advocate general  
(Case [C-487/21](#))

- With the fourth question it has referred for a preliminary ruling, the referring court asks the Court whether the concept of 'information' in the third sentence of Article 15(3) of the GDPR refers only to the 'personal data undergoing processing' referred to in the first sentence of that paragraph or whether, in addition to those, it also includes the information referred to in Article 15(1)(a) to (h) (fourth question under (a)) or even other information such as, for example, metadata about data (fourth question under (b)).
- Conclusion of the Advocate general:
- The concept of "information" in the third sentence of Article 15(3) of Regulation 2016/679 **must be interpreted as referring exclusively to the "copy of personal data undergoing processing" referred to in the first sentence of that paragraph.'**

# Limits and restrictions

- The right to obtain a copy shall not adversely affect the rights and freedoms of others (e.g. trade secrets, intellectual property, rights of other data subjects)
- Applying Art. 15(4) should not result in refusing the data subject's request altogether; it would only result in leaving out or rendering illegible those parts that may have negative effects for the rights and freedoms of others.



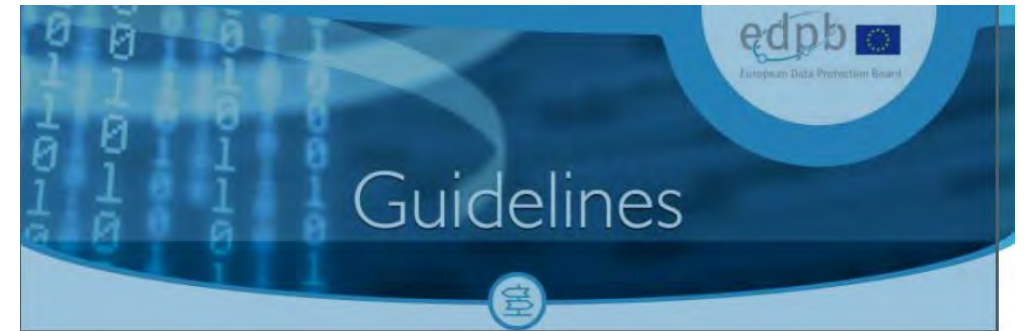
**Guidelines 01/2022 on data subject rights - Right of access**

**Version 1.0**

**Adopted on 18 January 2022**

# Security!

- the controller is always obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing
- Encryption is paramount, but access to data must be guaranteed



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

**Version 1.0**

**Adopted on 18 January 2022**

# Can DSR become a threat?

## GDPR: When the Right to Access Personal Data Becomes a Threat

Luca Bufalieri, Massimo La Morgia, Alessandro Mei, Julinda Stefa  
Department of Computer Science, Sapienza University of Rome, Italy

Email: bufalieri.1430586@studenti.uniroma1.it, {lamorgia, mei stef}@di.uniroma1.it

*Abstract*—After one year since the entry into force of the GDPR, all web sites and data controllers have updated their procedure to store users' data. The GDPR does not only cover how and what data should be saved by the service providers, but it also guarantees an easy way to know what data are collected and the freedom to export them.

In this paper, we carry out a comprehensive study on the right to access data provided by Article 15 of the GDPR. We examined more than 300 data controllers, performing for each of them a request to access personal data. We found that almost each data controller has a slightly different procedure to fulfill the request and several ways to provide data back to the user, from a structured file like CSV to a screenshot of the monitor. We measure the time needed to complete the access data request and the completeness of the information provided. After this phase of data gathering, we analyze the authentication process followed by the data controllers to establish the identity of the requester. We find that 50.4% of the data controllers that handled the request, even if they store the data in compliance with the GDPR, have flaws in the procedure of identifying the users or in the phase of sending the data, exposing the users to new threats. With the undesired and surprising result that the GDPR, in its present deployment, has actually decreased the privacy of the users of web services.

*Index Terms*—GDPR, Law Compliance, Privacy, Data Controllers, Web services

to a data controller. In our study, we target 334 of the most popular web sites according to the Alexa ranking. For the best of our knowledge, we are the first to conduct a comprehensive study on this topic with a world distribution of web sites, so our finding are also useful to refine previous works that took into account only one phase of the SAR [2], or used less rigorous methodologies to select the organizations [3], or could be biased by the small set of data controllers put under the lens [4].

We find that 19.6% of privacy policy pages are not compliant with the actual regulation. Then, we inquiry all the targeted web sites requiring our personal data. We study how the collectors identify the requester, we collect the response, and monitor the response time. In the end, we obtain our personal data from almost 65% of the targeted web sites, with a average time to fulfill the request of 16.4 days. Lastly, we checked the procedures used by the data controllers to fulfill the request. In this phase, we find several flaws that affect more than 32% of targeted data controller, and that could transform a fundamental right into a new and unpleasant threat.

This paper makes the following contributions:

- **World-wide snapshot:** We makes a world-wide snapshot of the actual deployment of the GDPR. We report on the

Blackhat USA 2019 Whitepaper

James Pavur and Casey Knerr

## GDPArrrrr: Using Privacy Laws to Steal Identities

James Pavur\*  
DPhil Researcher  
Oxford University

Casey Knerr  
Security Consultant  
Dionach LTD

# DSR and law enforcement directive

# DSR & Directive 2016/680

---

ARTICLE 29 DATA PROTECTION WORKING PARTY



17/EN  
WP 258

Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)

Adopted on 29 November 2017

## Recommendations of the WP29

1. The Directive provides for a new architecture of the rights of data subjects, the principle being that they have a right to information, access, rectification, erasure or restriction of processing, unless these rights are restricted. Such restrictions shall only be possible where they constitute a necessary and proportionate measure and interpreted in a restrictive manner. Where these rights will have been restricted, Member States shall provide for the possibility for data subjects to exercise their rights through the competent supervisory authority which constitutes an additional safeguard for the data subjects.
2. The Directive states that Member States must provide for data subjects to have the right to obtain confirmation of processing and access to personal data being processed from the controller. The Directive does not allow for blanket restrictions to data subject rights.



# DSR & EUROPOL REGULATION



EUROPEAN DATA PROTECTION SUPERVISOR

## Decision of the European Data Protection Supervisor in complaint case 2020-0908 against the European Union Agency for Law Enforcement Cooperation (Europol)

Search the site [Donate](#)

EDRi [About us](#) [What we do](#) [Take action](#)

[Home](#) » [Resources](#) » [Rather delete than comply: how Europol snubbed data subject rights](#)

### Rather delete than comply: how Europol snubbed data subject rights

On 8 September 2022, the European Data Protection Supervisor (EDPS) issued a decision ordering the EU law enforcement agency, Europol, to give Dutch activist Frank van der Linde access to the personal data the agency holds on him following a two-year investigation by the data protection watchdog. Findings of the inspection reveal that Europol tried to cover up the traces of the data processing and to avoid complying with the data access request by deleting van der Linde's data.

By EDRi · September 28, 2022

# DSR in the context of the European Data Strategy and the Digital services package

# Enhanced portability?

Digital Markets Act  
(REGULATION (EU)  
2022/1925)

- provide effective portability of data generated through the activity of a business user or end user –applies to gatekeepers;

Data governance Act  
(REGULATION (EU)  
2022/868)

- Data intermediation services (providers of secure environment for individual and companies to share data)
- Personal data spaces (data wallets) for individuals to share their data

Data Act

- Measures to allow users of connected devices to gain access to data generated by them (freeing IoT data)
- Reinforced data portability right, both for personal and non-personal data

Questions?





## Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2

Avv. Giovanni Battista Gallus – [gallus@array.law](mailto:gallus@array.law)

---

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

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

Mikołaj Otmianowski

Milan, 17 April 2023



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

# About Mikolaj

Training of Lawyers on  
EU Law relating to Data  
Protection 2

 #TRADATA2

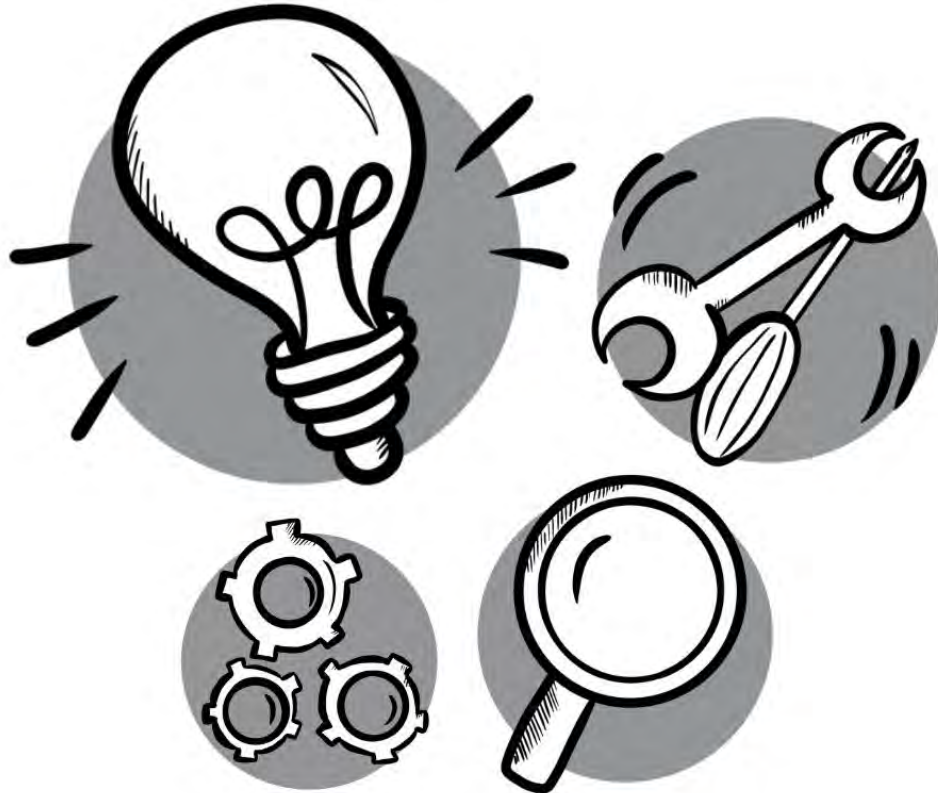
I am helping  
privacy teams  
to simplify their  
life and save time



# The Data Protection “package”

- 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]
- 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 2016/681/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]

# Scope



- protection of processing of personal data by competent authorities (art. 2)
  - for the purposes of the prevention, investigation, detection or prosecution of criminal offences or
  - the execution of criminal penalties
  - the safeguarding against and the prevention of threats to public security (art.1)
- competent authority' means (art. 3)
  - any public authority competent
  - any other body or entity entrusted by Member State law to exercise public authority and public powers

# GDPR vs LED

GDPR	Directive 680/2016
General provisions	General provisions
Principles	Principles
Rights of the data subject	Rights of the Data Subject
Controller and processor	Controller & Processor
General Obligations	General Obligations
Security	Security
DPIA and prior consultation	
Data Protection Officer	Data Protection Officer
Codes of conduct and certification	
Transfers of personal data to third countries or international organisations	Transfers of Personal data D to third countries
Independent supervisory authorities	Independent Supervisory Authorities
Cooperation and consistency	Cooperation
Remedies, liability and penalties	Remedies, Liability & Penalties
Provisions relating to specific processing situations	
Delegated acts and implementing acts	
Final provisions	Final Provisions

## GDPR = LED

implement appropriate technical and organization measures & demonstrate processing in accordance with Directive (19 LED)

implement data protection by design and by default (20)

use Processors with sufficient guarantees & act only on instructions from Controller (22)

maintain a record of processing activities (24)

cooperate with the Supervisory Authority (26)

carry out a data protection impact assessment - when high risk to the rights and freedoms of natural persons (27)

consult the supervisory authority in advance (cases listed in 28)

implement appropriate technical and organization measures to ensure a level of security appropriate to the risk, especially for special categories of PD referred to in art. 10 (29)

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)

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)

designate a DPO according to art. 32

respect the conditions defined for the transfer of personal data to third countries or to international organizations (art. 35 and following).

## GDPR ≠ LED

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

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)

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 right to rectification or erasure of personal data (16)

# The Polish perspective

- Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości z dnia 14 grudnia 2018 r. (Dz.U. z 2019 r. poz. 125)
- The provisions of the Act **do not apply** to the protection of personal data:
  - 1) contained in the files of cases or activities or recording devices, including those created and processed with the use of IT techniques (...)
  - 2) processed in connection with ensuring national security, including as part of the implementation of statutory tasks of the Internal Security Agency, Foreign Intelligence Agency, Military Counterintelligence Service, Military Intelligence Service and the Central Anti-Corruption Bureau.



# ROPA and risk assessment in Excel

Training of Lawyers on  
EU Law relating to Data  
Protection 2

#TRADATA2

WIDOK CHRONIONY **Ostrożnie — ten plik pochodzi z lokalizacji internetowej i może zawierać wirusy. Jeśli nie ma konieczności jego edytowania, bezpieczniej jest pozostać w widoku chronionym.** Włącz edytowanie

Dyrektor Szkoły

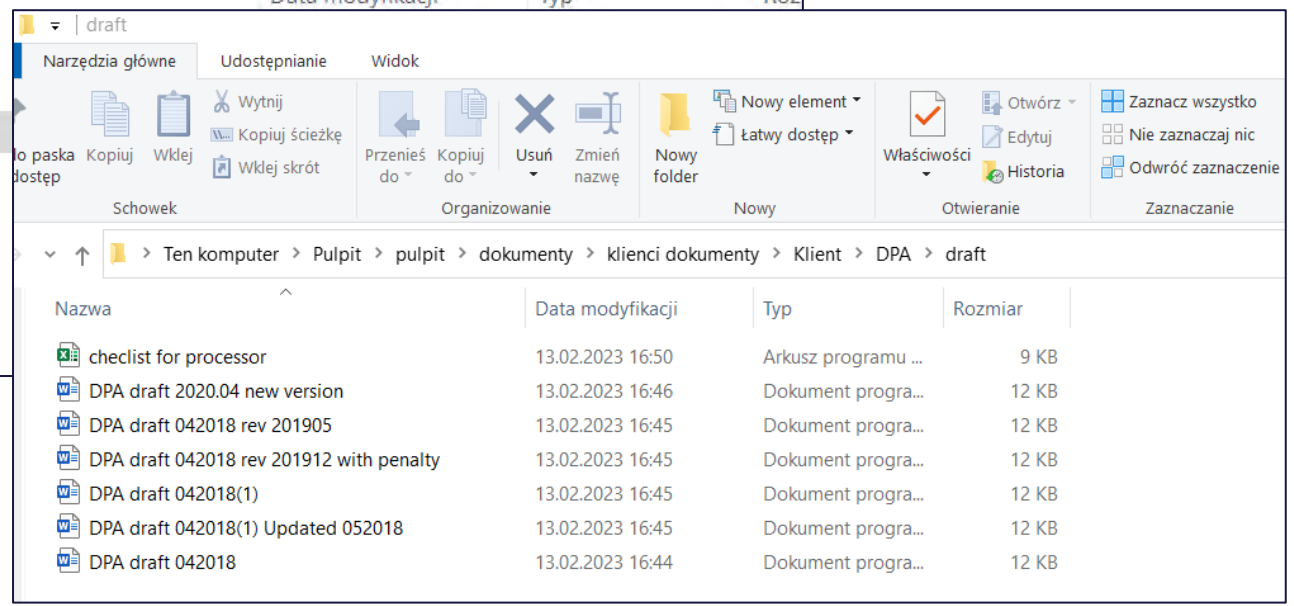
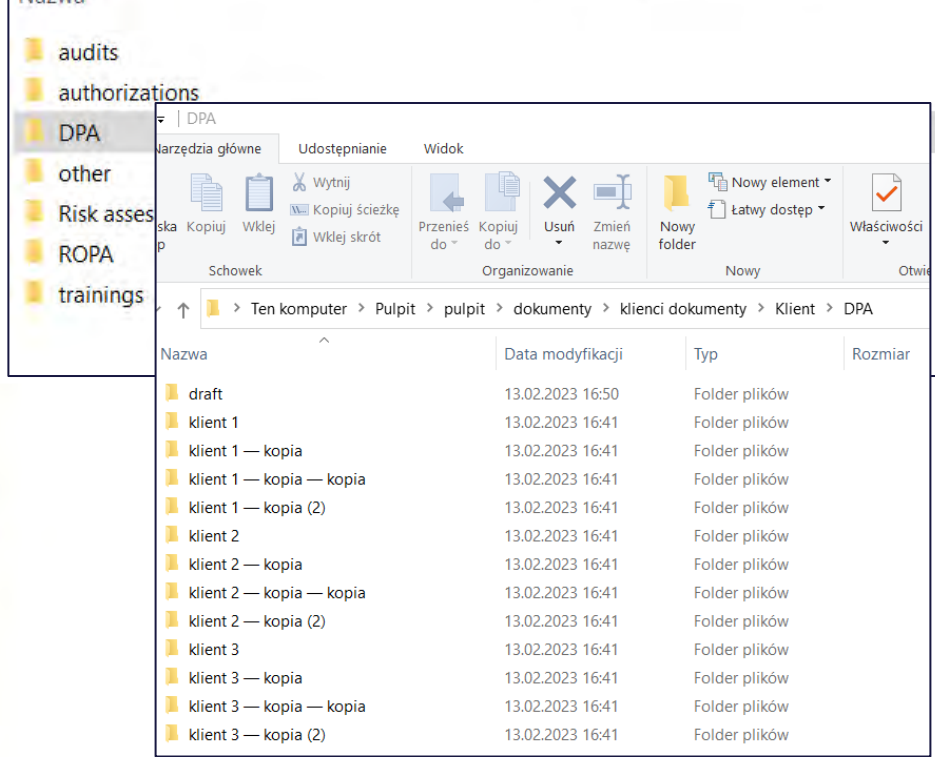
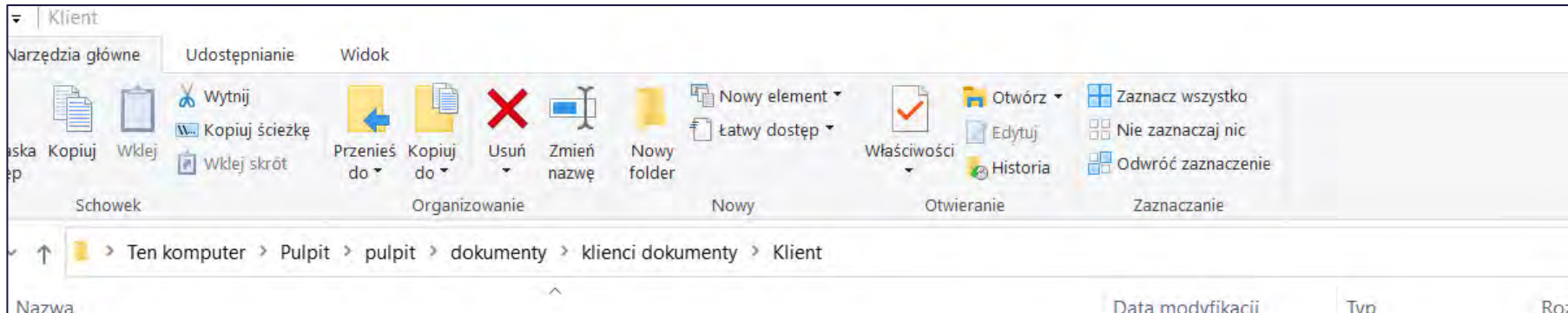
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Selekcja pracowniczych kandydatów do zatrudnienia	Dyrektor Szkoły	Selekcja pracowniczych kandydatów do pracy	Artykuł 30 ust. 1 pkt b	Artykuł 30 ust. 1 pkt c	Artykuł 30 ust. 1 pkt d	Artykuł 30 ust. 1 pkt e	Artykuł 30 ust. 1 pkt f	Artykuł 30 ust. 1 pkt g	Artykuł 30 ust. 1 pkt h	Artykuł 30 ust. 1 pkt i	Artykuł 30 ust. 1 pkt j	Artykuł 30 ust. 1 pkt k	Artykuł 30 ust. 1 pkt l	Artykuł 30 ust. 1 pkt m	Artykuł 30 ust. 1 pkt n

B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Selekcja pracowniczych kandydatów do zatrudnienia	Dyrektor Szkoły	Selekcja pracowniczych kandydatów do pracy	Artykuł 30 ust. 1 pkt b	Artykuł 30 ust. 1 pkt c	Artykuł 30 ust. 1 pkt d	Artykuł 30 ust. 1 pkt e	Artykuł 30 ust. 1 pkt f	Artykuł 30 ust. 1 pkt g	Artykuł 30 ust. 1 pkt h	Artykuł 30 ust. 1 pkt i	Artykuł 30 ust. 1 pkt j	Artykuł 30 ust. 1 pkt k	Artykuł 30 ust. 1 pkt l	Artykuł 30 ust. 1 pkt m	Artykuł 30 ust. 1 pkt n

B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Selekcja pracowniczych kandydatów do zatrudnienia	Dyrektor Szkoły	Selekcja pracowniczych kandydatów do pracy	Artykuł 30 ust. 1 pkt b	Artykuł 30 ust. 1 pkt c	Artykuł 30 ust. 1 pkt d	Artykuł 30 ust. 1 pkt e	Artykuł 30 ust. 1 pkt f	Artykuł 30 ust. 1 pkt g	Artykuł 30 ust. 1 pkt h	Artykuł 30 ust. 1 pkt i	Artykuł 30 ust. 1 pkt j	Artykuł 30 ust. 1 pkt k	Artykuł 30 ust. 1 pkt l	Artykuł 30 ust. 1 pkt m	Artykuł 30 ust. 1 pkt n

B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Selekcja pracowniczych kandydatów do zatrudnienia	Dyrektor Szkoły	Selekcja pracowniczych kandydatów do pracy	Artykuł 30 ust. 1 pkt b	Artykuł 30 ust. 1 pkt c	Artykuł 30 ust. 1 pkt d	Artykuł 30 ust. 1 pkt e	Artykuł 30 ust. 1 pkt f	Artykuł 30 ust. 1 pkt g	Artykuł 30 ust. 1 pkt h	Artykuł 30 ust. 1 pkt i	Artykuł 30 ust. 1 pkt j	Artykuł 30 ust. 1 pkt k	Artykuł 30 ust. 1 pkt l	Artykuł 30 ust. 1 pkt m	Artykuł 30 ust. 1 pkt n

# Archive in Windows



# „Yes, we have implemented the GDPR”

- Long, unclear obligation information
- Consent as a main ground on everything
- DPA everywhere
- General trainings
- No process
- No audit
- Trust to subcontractors based on their statement
- Long not verified questionnaire



# No conclusion, no comparison

Training of Lawyers on  
EU Law relating to Data  
Protection 2

#TRADATA2

Actualizacja pakietu Office. Aby być na bieżąco z aktualizacjami zabezpieczeń...

Luty - 2 POŁOWA	lut.02		
data emisji	termin obowiązywania	produkt z	temat
		billboard	
		billboard	fb_panel
			fb_wc_kompakt
		petarda	2012672_fb_kompasor

Patologii Słuch w sierpniu 2022

Model licencji 500 mc/5000 n

W ramach opłaty:

- helpdesk (rozwiązywanie problemów z działaniem aplikacji) – SLA do 48 godzin w dni robocze;
- Usługi dodatkowe (opcja)
  - dedykowane szkolenie on-line wprowadzające zamknięte dla organizacji klienta do 10 godzin (dla organizacji klienta, na jego przyładach) do 12 osób: 8.000 PLN + VAT; w przypadku szkolenia w biurze poza Warszawą koszty do ustalenia;
  - merytoryczne wsparcie konsultanta (spotkanie online): 1.800 PLN/za dzień roboczy lub 250 PLN/godzinę;
  - uzupełnienie danych w RED INTO GREEN – wyznaczone na żądanie;

Warunki formalne

- Platność za licencje z góry za wybrany okres;
- Platność w terminie 14 dni od daty otrzymania FV, za usługi dodatkowe świadczone w ramach konsultingu faktury będą wystawiane po zakończeniu miesiąca;
- Do wszystkich cen należy dodać podatek VAT;
- W przypadku umów z platnością miesięczną umowa jest podpisywana na czas nieokreślony.

webinar	06.02.godz.11.00	07.02.godz.18.00	08.02.godz.11.00	09.02.godz.18.00	10.02.godz.11.00
webinar 1	06.02.godz.11.00	07.02.godz.18.00	08.02.godz.11.00	09.02.godz.18.00	10.02.godz.11.00
webinar 2	13.02.godz.11.00	14.02.godz.18.00	15.02.godz.11.00	16.02.godz.18.00	17.02.godz.11.00
webinar 3	20.02.godz.11.00	21.02.godz.18.00	22.02.godz.11.00	23.02.godz.18.00	24.02.godz.11.00
webinar 4	27.02.godz.11.00	28.02.godz.18.00	1.03.godz.11.00	2.03.godz.18.00	3.03.godz.11.00
webinar 5	06.03.godz.11.00	07.03.godz.18.00	08.03.godz.11.00	09.03.godz.18.00	10.03.godz.11.00
webinar 6	13.03.godz.11.00	14.03.godz.18.00	15.03.godz.11.00		
webinar 7			15.03.godz.18.00	16.03.godz.11.00	17.03.godz.14.00
webinar 8	20.03.godz.11.00	21.03.godz.18.00	22.03.godz.11.00		
webinar 9			22.03.godz.11.00	23.03.godz.18.00	24.03.godz.11.00
webinar 10	27.03.godz.11.00	28.03.godz.18.00	29.03.godz.11.00		

## Cyberbezpieczeństwo compliancowo:

- Zarządzanie ryzykiem, w tym analiza ryzyka
  - Bezpieczeństwo łańcucha dostaw
  - Zarządzanie podatnościami (KSC2 i NIS2)
- Zarządzanie incydentami, w tym zgłoszenie naruszeń
  - Zgłoszenie do CERT
- Zarządzanie ciągłością działania
- Monitorowanie, audyt i testowanie
- Polityka bezpieczeństwa
- Szkolenia i baza wiedzy

## Raporty-ważne narzędzie dla organizacji klienta

Wysokopozycyjowe rezultaty na tle skali ryzyka

Skala ryzyka oraz Skala poziomu ryzyka, we wszystkich ocenianych kombinacjach

Udział poszczególnych kategorii ryzyka we wszystkich ocenianych kombinacjach

Pobranie rzeczy

Nazwa	Wielkość	Rodzaj
Kontratacja RODO DAPR-ica	1 KB	Plik tekstowy
webinar_8202145679-ica	2 KB	Plik tekstowy
film_glowny.pptx	3,0 MB	Prezentacja (pptx)
5 milow na tema...webinar_IB.splix	5,4 MB	Prezentacja (pptx)
5 milow na tema...inar_w_K.pptx	4,8 MB	Prezentacja (pptx)
5 milow na tema...ow webinar.pptx	1 MB	Prezentacja (pptx)
Administrator, W...sly 35 04.pptx	3,8 MB	Prezentacja (pptx)
Administrator, W...ministrator.pptx	9 MB	Prezentacja (pptx)
Analiza ryzyka a...ony danych.pptx	1,8 MB	Prezentacja (pptx)
Analiza Ryzyka L...aMO (1).pptx	2,7 MB	Prezentacja (pptx)
Analiza Ryzyka L...aMO (1).pptx	2,6 MB	Prezentacja (pptx)
Analiza Ryzyka L...aMO (1).pptx	1,6 MB	Prezentacja (pptx)
Analiza Ryzyka L...aMO (1).pptx	1,4 MB	Prezentacja (pptx)
analiza ryzyka L...ryka_MacO.pptx	4,7 KB	Prezentacja (pptx)
Aplikacja DAPR...a do zmiany.pptx	3,4 MB	Prezentacja (pptx)
Aplikacja do Ana...ka RODO_2.pptx	1,1 MB	Prezentacja (pptx)
RO DAPR.pptx	7,85 KB	Prezentacja (pptx)
DAPR - Oferta U...2021-06-16.pptx	269 KB	Prezentacja (pptx)
DAPR - Prezent...21-08-31.1.pptx	849 KB	Prezentacja (pptx)
DAPR - Prezent...zsolnowa.pptx	2,3 MB	Prezentacja (pptx)
DAPR -AML - v1.pptx	3,6 MB	Prezentacja (pptx)
DAPR -AML - v2.pptx	3,6 MB	Prezentacja (pptx)
DAPR dla podw...inowanego.pptx	7,82 KB	Prezentacja (pptx)
Decathlon_aplik...ryka RODO.pptx	1,1 MB	Prezentacja (pptx)

Cykl godzinnych szkoleń dotyczących DEZINFORMACJI.

Zapraszamy Cię do zapisów na DRUGIE szkolenie z cyklu: DEZINFORMACJA czyli zamierzone działanie, którego celem jest sfałszowanie lub zaburzenie przekazu informacyjnego, by osiągnąć własne korzyści polityczne, społeczne, finansowe, militarne itd.

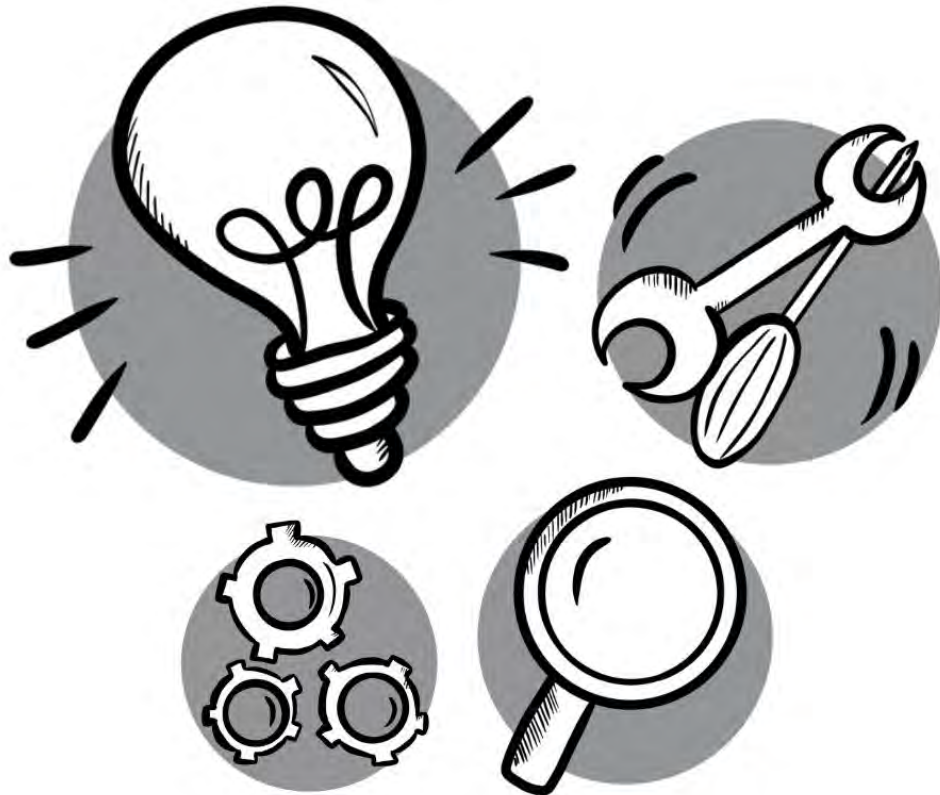
Ten cykl szkoleń, pomoże Ci zrozumieć poniższe zagadnienia:

- Dezinformacja – wprowadzenie, najniższe informacje
- Jak chronić się przed dezinformacją?
- Wojna informacyjna toczy się obok nas. Jak ją dostrzec?
- Wojna w Ukrainie – czas żniw dla dezinformacji
- ABC dezinformacji – podejście praktyczne.

Tematem osmy webinarium jest „Wojna informacyjna toczy się obok nas. Jak ją dostrzec?”

- Wojna informacyjna toczy się obok nas. Jak ją dostrzec?
  - Założenie: Ws współczesnym świecie umowy o stałe toczące się wojnie informacyjnej. Skąd to pojęcie i dlaczego jest szczególnie ważne w obliczu wojny za wschodnią granicą? Jak budowane są linie dezinformacyjne i do czego mogą prowadzić? Jakie próby manipulowania odbiorcami są podejmowane?
  - Uczestnik uzyska odpowiedzi na pytania:
    - Przykłady linii dezinformacyjnych
    - Do czego może prowadzić dezinformacja

# Implications – after 5 years



- The Excel is hard to open, use or update
- Documents become unreadable
- Lack of transparency and order
- No reports or analysis
- Lack or low budget on the GDPR
- One DPO is enough for organization
- Tones of outdated autorisation, DPA and other.

Fear of accounting for the performance of the function for 5 years

# Time for software - NOW

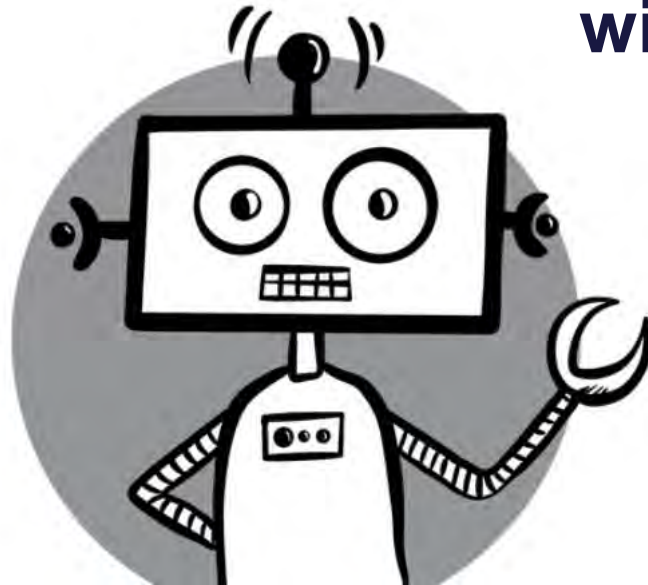
- Everybody searches for software
- Many people have the belief that there is nothing
  - „I need to clean my desk”
- Fear of the end of cooperation – „I have nothing to give!”



# How to make the GDPR management easier?



- Software support
- Engage more business owners
- **Connect the GDPR with cyber security**

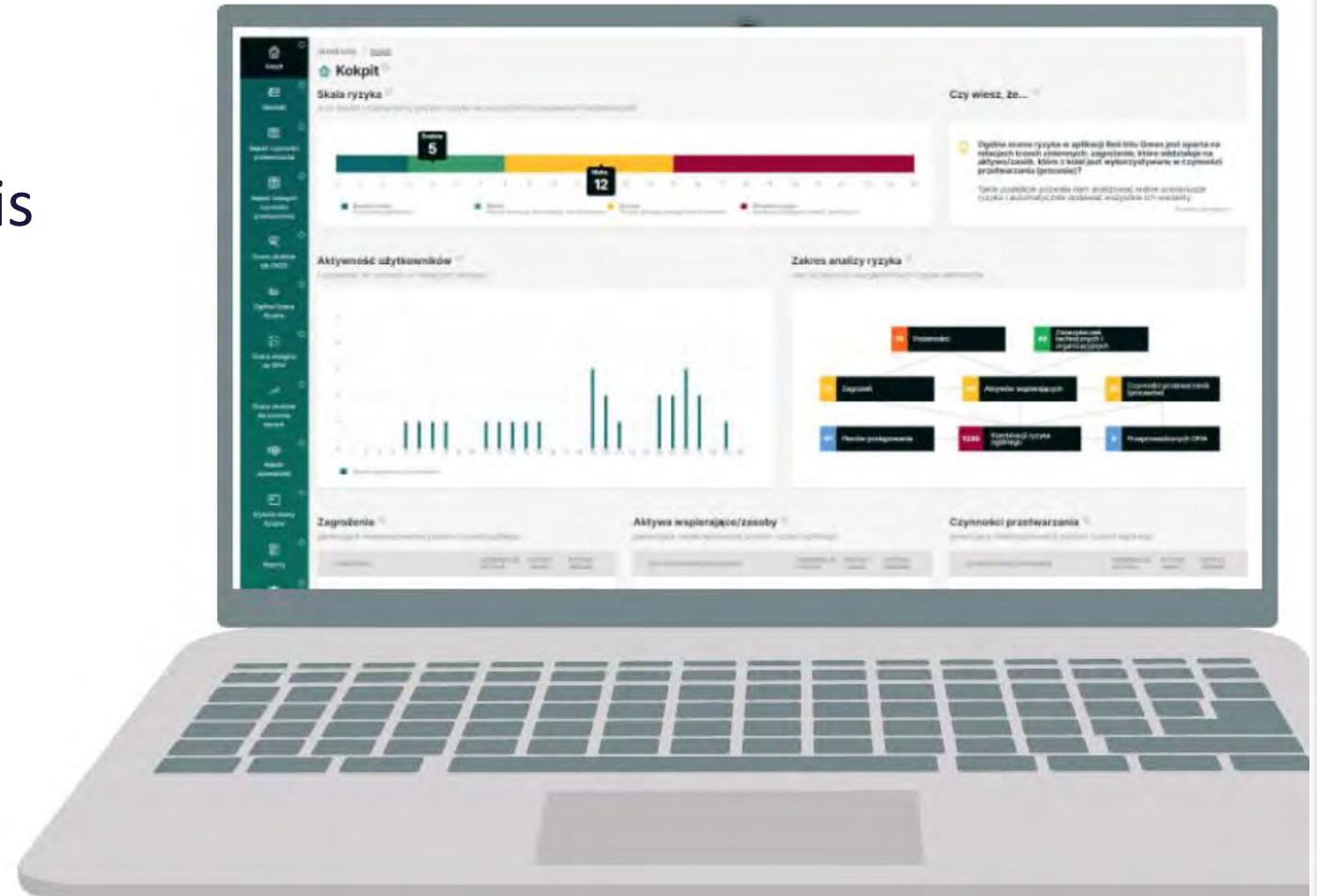


# What the GDPR software should provide

Training of Lawyers on  
EU Law relating to Data  
Protection 2

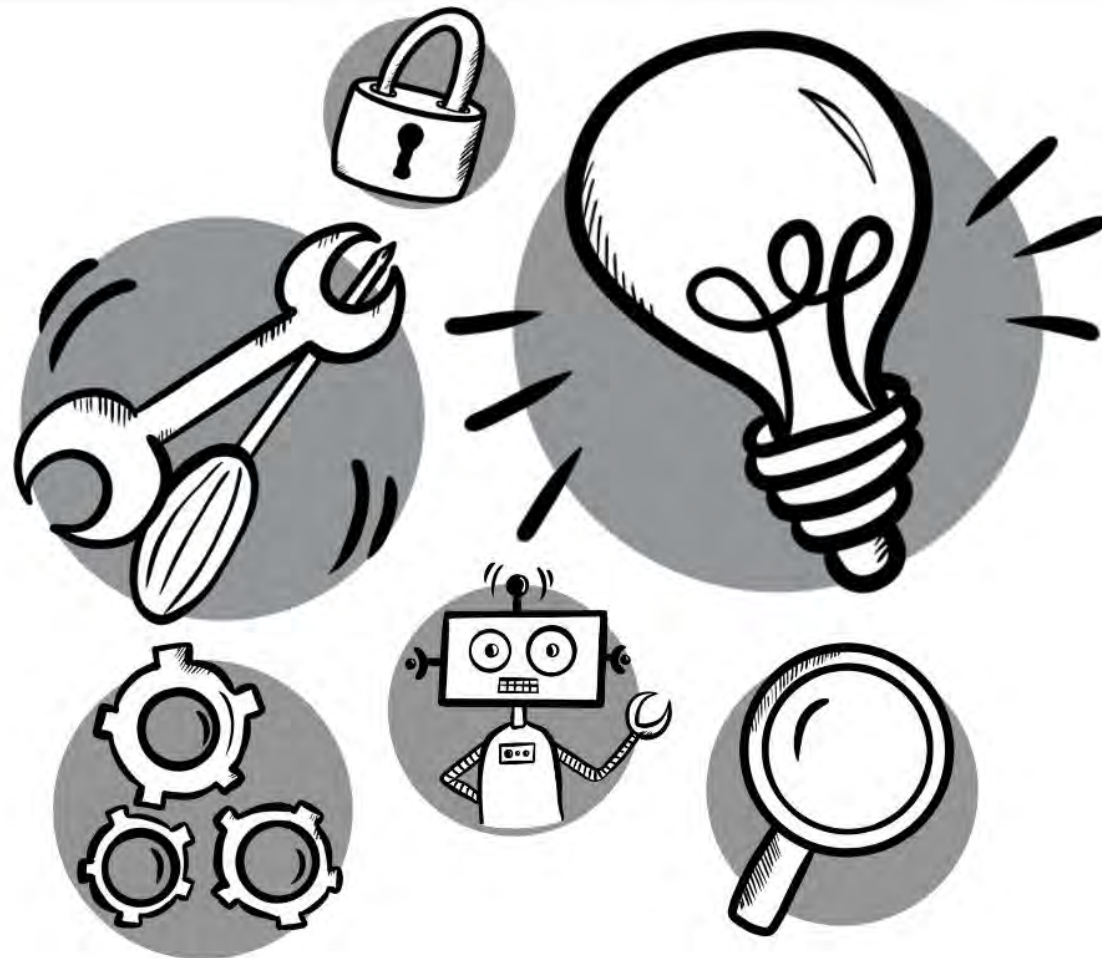
#TRADATA2

- registry management module
- module to manage risk analysis and DPIA
- audit management module
- training modules
- breach assessment
- reports
- check list and plans



# At the end

- All the GDPR issues are in one place
- ROPA is a map of the processes and the GDPR
- Clarity, transparency, linkage of information
- We can combine work done for the GDPR with cyber
- One team working together: IT, DPO and Legal Dept.
- The GDPR is a part of protection of the company
- The whole picture is security and processes, GDPR is a part of security



# DPO

1. see a whole picture
2. role is important as combiane with cyber
3. teamwork
4. software support
5. easier to update data and compare it



DPO should  
be happy!

# List of polish applications for GDPR

1. <https://redintogreen.dapr.pl/>
2. <https://store.pwc.pl/pl/produkty/program-do-rodo>
3. <https://gdprrisktracker.pl/>
4. <https://gdpstandard.com/pl/>
5. <https://odo24.pl/dr-rodo#cennik>
6. <https://inspektor365.pl/>
7. <https://rodo-online.eu/>
8. <https://kryptos72.com/>
9. <https://rodoprotektor.pl/>
10. <https://iodinspektor.pl/>
11. <http://dlaiod.pl/program-rodo/>
12. <https://ioda.legal/>
13. <https://sodo.com.pl>

Training of Lawyers on  
EU Law relating to Data  
Protection 2

 #TRADATA2



**Mikołaj Otmianowski**



 **RED INTO GREEN**  
GDPR compliance tool by DAPR

**Thank you for your attention**

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

The consent under the GDPR







Nadia Arnaboldi

Milan, 17 April 2023



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

# Agenda

-  Legal provisions and soft laws
-  The notion of consent
-  Elements of valid consent
-  Proof of consent and withdrawal of consent
-  Children's consent
-  Courts' rulings and SA's decisions



## Legal provisions and soft laws

- **Charter of fundamental rights:** Articles 7 and 8
- **GDPR:** Articles 4(11), 7, 8 and recitals 32, 33, 38, 42 and 43
- **WP29/EDPB guidelines and opinions:** EDPB Guidelines 05/2020 on consent adopted on 4 May 2020 (see also WP29 opinion 15/2011)

## Legal provisions and soft laws

### Charter of fundamental rights

#### Article 7 Respect for private and family life

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

#### Article 8 Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such **data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law**. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority

## Notion of consent

- **Consent is one of the six lawful bases** to process personal data and it is on the controller to assess if consent is an appropriate lawful ground for a particular processing operation (article 6(1)(a))
- The data subject shall be always offered **control over his or her personal data and a genuine choice** if to accept or refuse consent without detriment
- Even if the data subject has given consent to the processing, the **controller's obligation to comply** with all the provisions of the GDPR, in particular the data processing principles, and the national data protection provisions **remains**
- **Consent in the GDPR = consent in the e-Directive**





## Notion of consent

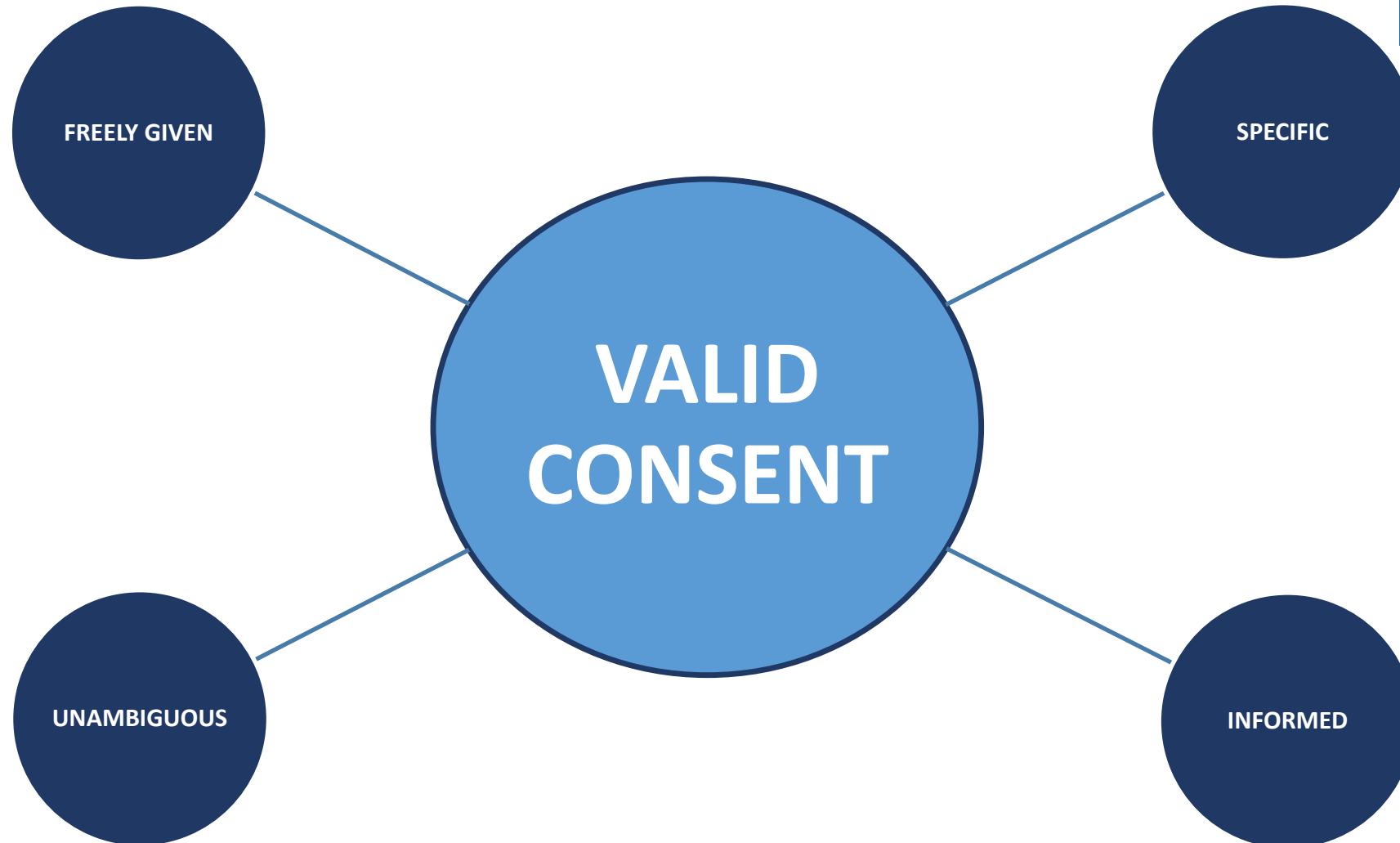
### Article 4(11) GDPR

*“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 a valid consent

---



## Elements of a valid consent

---

### 'Freely given'

'Free' implies **real choice and control** for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.



Imbalance of power



Conditionality



Granularity



Detriment

## Elements of a valid consent

---

**'Imbalance of power'**



```
graph LR; A["'Imbalance of power'"] --> B["Recital 43"]; A --> C["EDPB Guidelines"];
```

### Recital 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'*

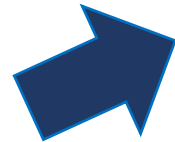
### EDPB Guidelines

*'It is unlikely that **public authorities** can rely on consent for processing as there is often a clear imbalance of power. An imbalance of power can also occur in the **employment context**. However, the **use of consent** as legal bases by public authorities or employer **is not totally excluded** as it depends on the circumstances (see EDPB examples). Imbalance of power may occur in other situations'*

# Elements of a valid consent

---

## 'Conditionality'



### Recital 43

*'Consent is presumed not to be freely given (...) 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'*



### Article 7(4)

*'When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'*



### EDPB Guidelines

EDPB underlines that *'the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract'*

# Elements of a valid consent

---

## 'Granularity'



### Recital 43 and Recital 32

*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 (...). According to recital 32 'Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them'*

### Article 6(1)(a)

*The data subject has given **consent** to the processing of his or her personal data **for one or more specific purposes***

### EDPB Guidelines

EDPB underlines that *the data subjects should be free to choose which purpose they accept. If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a **lack of freedom***

# Elements of a valid consent

---

## 'Detriment'



```
graph LR; A["'Detriment'"] --> B["Recital 42"]; A --> C["EDPB Guidelines"]; B --- C;
```

### Recital 42

*'Consent should not be regarded as freely given if the data subject (...) is unable to refuse or withdraw consent without detriment'*

### EDPB Guidelines

#### Examples of detriment

- *'withdrawing consent does not lead to any costs for the data subject',*
- *'deception, intimidation, coercion or significant negative consequences if a data subject does not consent,*
- *'the performance of a service being downgraded to the detriment of the user'*

## Elements of a valid consent

---

### **'Specific'**

*The data subject has given **consent** to the processing of his or her personal data **for one or more specific purposes (article 6(1)(a)).***

*According to the **EDPB guidelines 'to comply with the element of 'specific' the controller must apply':***



**Purpose specification as a  
safeguard against function  
creep**



**Granularity in  
consent requests**



**Clear separation of information  
related to obtaining consent for data  
processing activities from information  
about other matters**

# Elements of a valid consent

---

## **‘Informed’**

***‘Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory, and consent will be an invalid basis for processing’ (EDPB Guidelines).***

# Elements of a valid consent

---

## Minimum information required for a valid consent (EDPB Guidelines)

→ **Controller's identity**

→ The **purpose of each of the processing operations** for which consent is sought

→ What **type of data** will be collected and used

→ The existence of the **right to withdraw consent**

→ Information about the **use of the data for automated decision-making** in accordance with article 22(2)(c) where relevant

→ The **possible risks of data transfer** due to the absence of an adequate decision and of appropriate safeguards as described in article 46

# Elements of a valid consent

---

## 'Unambiguous indication of wishes'

*'consent requires a **statement** from the data subject or a **clear affirmative act**, which means that it must always be given through an active motion or declaration' (EDPB Guidelines)*



## 'clear affirmative act'

the data subject must have taken a deliberate action, e.g. through a written statement, including by electronic means, or recorded oral statement



**Pre-ticked opt-in box is invalid.  
Data subject's silence or inactivity  
cannot be regarded as indication of  
choice**

# Proof of consent and withdrawal of consent

---



## Article 7(1) GDPR

*‘the controller shall be able to **demonstrate that the data subject has consented** to processing of his or her personal data’*

### How to demonstrate the data subject’s consent?

- The GDPR does not prescribe a specific methodology to prove that valid consent has been obtained
- Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations (i.e. accountability)
- No specific time limit in the GDPR for how long consent will last but the EDPB recommends as a best practice to refresh consent at appropriate intervals

# Proof of consent and withdrawal of consent

---

## Article 7(3) GDPR

*‘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’*

### How withdrawing consent

- When consent is obtained via electronic means, data subject must be able to withdraw that consent equally as easily
- Controllers have an obligation to delete data processed on the basis of consent once the consent is withdrawn, if no other lawful basis justified the processing (e.g. further storage for legal purposes)
- No specific time limit in the GDPR for how long consent will last, but the EDPB recommends as a best practice to refresh consent at appropriate intervals

## Children's consent

---

The GDPR provides for specific data protection for minors by requiring, in general, that **any information or communication intended for minors use simple and clear language** that can be easily understood by this specific type of data subjects who are less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data (see article 12).

*‘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’ (Recital 38).*

# Children's consent

---

## Article 8 GDPR

- Where consent 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***
- Outside information society services, the age limit of 18 for the provision of valid consent remains

## Children's consent

- In **Italy**, Article 2-quinquies of Legislative Decree 196/2003 established **14 years as the minimum age** for expressing such consent, taken into account the Garante's recommendations (legal provisions set 14 as the age limit for exercising certain legal actions, such as the provisions on cyberbullying that allow children over the age of 14 to exercise the rights provided for their protection against acts of cyberbullying against them, or the right of children over the age of 14 to give their consent to adoption)



**Data controller must be aware of different national laws**

## Courts rulings and SA's decisions

---

### European Court of Justice

- **Case C-61/19 (Orange România SA):** Orange Romania concluded paper-based contracts for the provision of mobile telecommunication services with individual customers at business premises and asked to the customers copies of their identity documents to be annexed to those contracts. The content of those contracts included, inter alia, a statement of the fact that the customer had been informed of and had consented to the collection and storage and that the existence of the customers' consent had been established by the insertion of crosses in boxes in the written documentation evidencing the contract. However, Orange România has not provided evidence that, at the time the contracts were concluded, the customers concerned had made an informed choice as to the collection and storage of those copies. The Court has established that **consent given in the form of a preselected tick of a checkbox does not imply active behaviour on the part of the website use.**

# Courts rulings and SA's decisions

---

## Supreme Court



- **Section I, decision 1 June 2022, n. 17911:** A cooperative company made public the work performance of employees or worker-members in order to score them in an internal competition on the quality of work. The company argued that the workers had given specific consent to such processing of their personal data through the members' general meeting approving the internal competition 'Quality of Work'. According to the Supreme Court **consent is only valid if specifically and voluntarily given**, which precludes the assertion that the individual can consent by means of a majority resolution of the members' meeting. Consent to such invasive processing as making personal data relating to work available to the public and specifically targeting disciplinary findings cannot be derived from a majority vote.

## Courts rulings and SA's decisions

---

### Main recent Italian SA's decisions

- **Decision 11 April 2023 n. 114 (ChatGPT):** among others, consent as possible legal bases and requirement to develop a plan for age verification for children under 13
- **Decision 23 February 2023 n. 50:** acquisition of data subjects' list from third parties without the data subjects' consent
- **Decision 15 December 2022 n. 431:** telemarketing and teleselling without consent (article 130 of the Italian data protection code requires customer's consent)
- **Decision 15 December 2022 n. 429:** telemarketing and teleselling without consent
- **Decision 10 November 2022 n. 379:** Telemarketing without consent

## Courts rulings and SA's decisions

---

### Main recent Italian SA's decisions

- **Decision 30 June 2022 n. 238:** requirement of specificity and granularity of consent for **scientific research** purposes. As at the time of collection it is not possible to fully identify the specific purposes of the future studies, the initial consent given by the patient for future studies is not sufficient and the data subjects shall have to give their **consent in stages** after the approval of each specific future research projects (see also recital 33)
- **Decision 10 June 2021 n. 231 'Guidelines on cookies and other tracking tools':** Scrolling is per se unsuitable to obtain valid consent. Cookie wall is unlawful, except where the website enables a user to access equivalent contents or services without consenting to the installation and use of cookies. This will have to be assessed case by case and in the light of GDPR principles.

## Courts rulings and SA's decisions

---

### Italian SA's decisions

According with article 22(4) of Legislative decree 10 August 2018 n. 101, as from 25 May 2018, the Garante's decisions continue to apply insofar as they are compatible with the GDPR

- **E.g. Decision 4 July 2013 n. 330 'Guidelines on marketing and against spam':** obligation to obtain prior consent (*'A contracting party's consent to promotional activities can be regarded as freely given if it does not represent the default setting or if it does not translate – even only factually or implicitly – into a precondition to obtain the product or service being offered by the data controller'* and *'it is not acceptable that forms are made available where the consent checkbox is flagged by default'*), consent for marketing purposes, specific consent to communicate and/or transfer data to third parties for marketing purposes, written proof of consent for marketing purposes.

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

Transfers of personal data to third countries

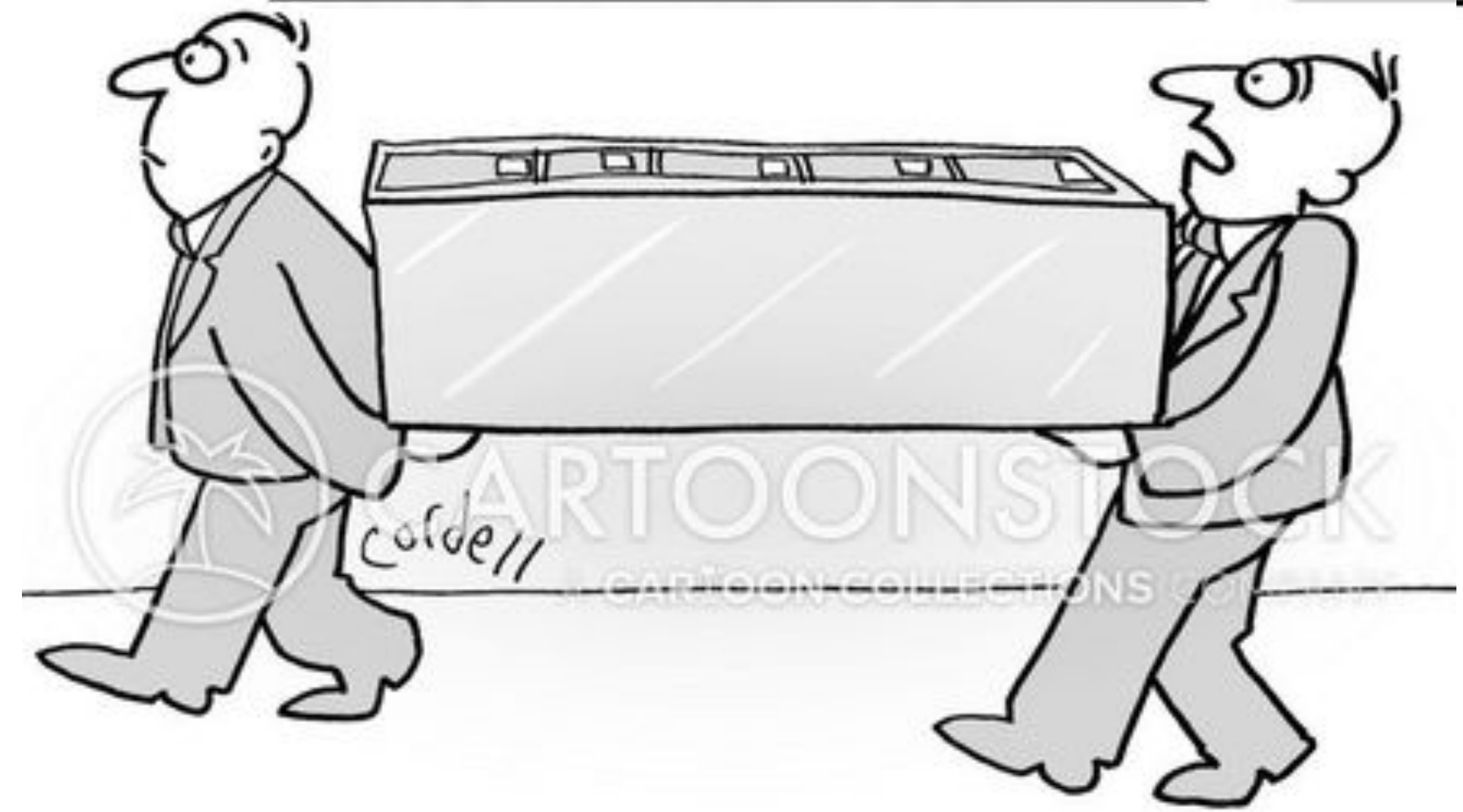
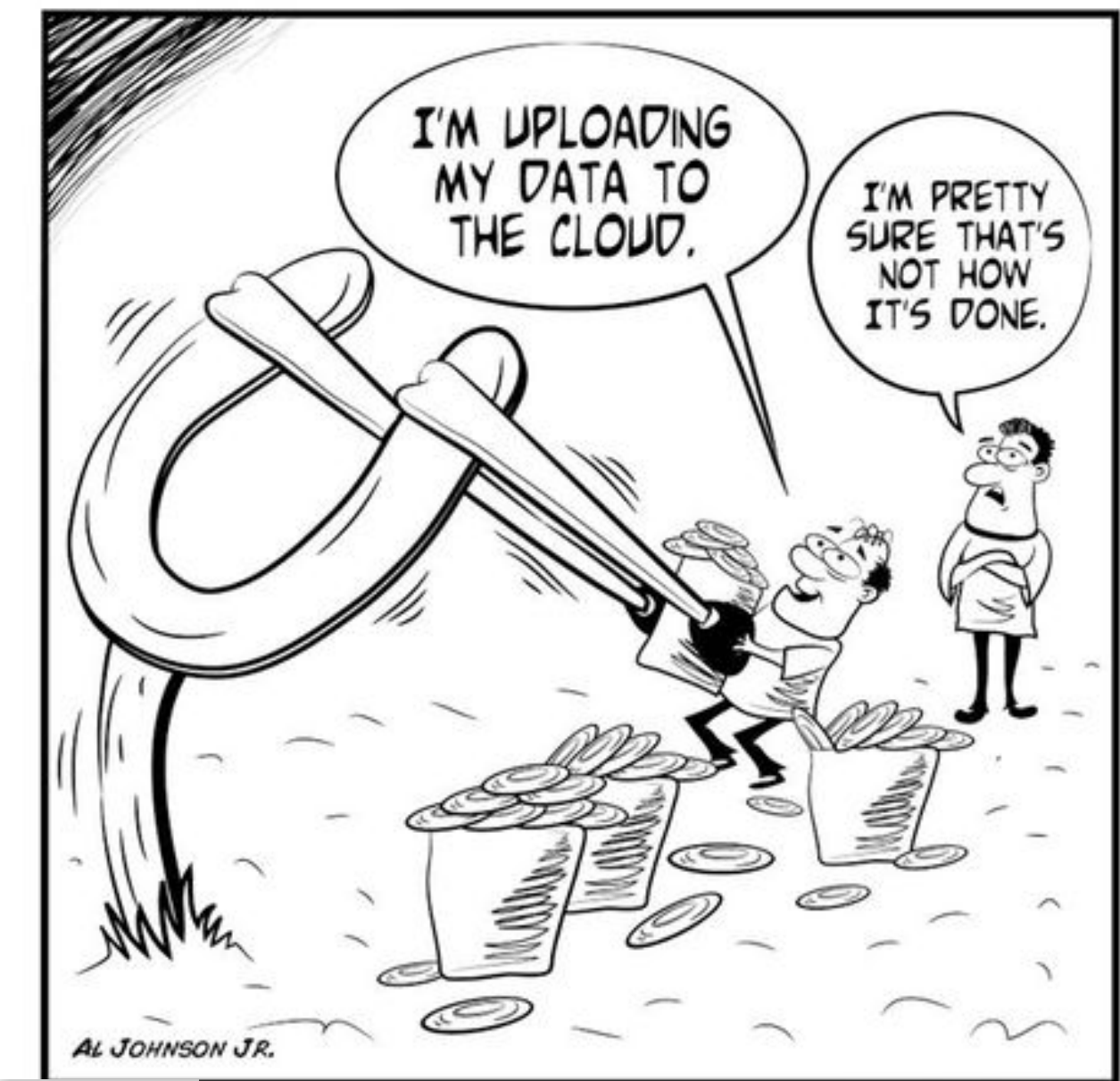
Nicola Fabiano

Milan, 17 April 2023



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

# Transfers of personal data to third countries or international organisations



“Surely there’s an easier way of moving files?”

# Transfers of personal data to third countries or international organisations

## CHAPTER V

**Article 44** - *General principle for transfers* (W101, W102)

**Article 45** - *Transfers on the basis of an adequacy decision* (W103, W107, W167-W169)

**Article 46** - *Transfers subject to appropriate safeguards* (W108, W109, W114)

**Article 47** - *Binding corporate rules* (W110, W167-W168)

**Article 48** - *Transfers or disclosures not authorised by Union law* (W115)

**Article 49** - *Derogations for specific situations* (W111-W114)

**Article 50** - *International cooperation for the protection of personal data* (W116)

*Is that regulation in the GDPR only in Chapter V?*

*No, see also Articles: 3 - 15(1)(c) - 30(1)(d) - 40(3) - 96 - Convention 108/1981 - Article 14*

# EDPB Guidelines n. 5/2021

## Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR - Adopted on 18 November 2021

Since the GDPR does not provide for a legal definition of the notion “transfer of personal data to a third country or to an international organisation”, it is essential to clarify this notion.

The EDPB has identified **the three following cumulative criteria** that qualify a processing as a transfer:

- 1) A controller or a processor **is subject to the GDPR for the given processing.**
- 2) This controller or processor (“exporter”) **discloses by transmission or otherwise makes personal data, subject to this processing, available to** another controller, joint controller or processor (“importer”).
- 3) **The importer is in a third country or is an international organisation, irrespective of whether or not** this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.

# EDPB Guidelines 5/2021 - 1<sup>st</sup> crit.

The **first criterion** requires that the processing at stake meets the requirements of Article 3 GDPR, i.e. that a controller or processor is subject to the GDPR for the given processing. This has been further elaborated on in the **EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)**.

It is worth underlining that controllers and processors, which are not established in the EU, may be subject to the GDPR pursuant to Article 3(2) for a given processing and, thus, will have to comply with Chapter V when transferring personal data to a third country or to an international organisation.

# EDPB Guidelines 5/2021 - 2<sup>nd</sup> crit.

The **second criterion** requires that there is a controller or processor disclosing by transmission or otherwise making data available to another controller or processor. These concepts have been further elaborated on in the **EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR**. It should, inter alia, be kept in mind that the concepts of controller, joint controller and processor 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. **A case-by-case analysis of the processing at stake and the roles of the actors involved is necessary.**

The **second criterion** implies that the concept of “*transfer of personal data to a third country or to an international organisation*” **only applies to disclosures of personal data** where two different (separate) parties (each of them a controller, joint controller or processor) are involved. In order to qualify as a transfer, there must be a controller or processor disclosing the data (the exporter) and a different controller or processor receiving or being given access to the data (the importer).

# EDPB Guidelines 5/2021 - 3<sup>rd</sup> crit.

The **third criterion** requires that the importer is geographically in a third country or is an international organisation, **but regardless of whether the processing at hand falls under the scope of the GDPR.**

# EDPB Guidelines 5/2021 - Conclusions

If all of the criteria as identified by the EDPB are met, there is a “transfer to a third country or to an international organisation”. Thus, a transfer implies that personal data are sent or made available by a controller or processor (exporter) which, regarding the given processing, is subject to the GDPR pursuant to Article 3, to a different controller or processor (importer) in a third country, regardless of whether or not this importer is subject to the GDPR in respect of the given processing.

As a consequence, the controller or processor in a “transfer” situation (according to the criteria described above) needs to comply with the conditions of Chapter V and frame the transfer by using the instruments which aim at protecting personal data after they have been transferred to a third country or an international organisation.

# General principles

# General principles

## Subjective scope

**Third country (non-EEA, and that is non-EU countries + Norway + Liechtenstein + Iceland)**

**«international organisation»**: means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries. - Art. 4(26)

**DIRECTIVE 2014/23/EU of the EUROPEAN PARLIAMENT and of the COUNCIL of 26 February 2014 on the Award of Concession Contracts**

*Article 6 § 4*

4. 'Bodies governed by public law' means bodies that have all of the following characteristics:

- (a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;
- (b) they have legal personality; and
- (c) they are financed, for the most part, by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those bodies or authorities; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law.

**DIRECTIVE 2014/24/EU of the EUROPEAN PARLIAMENT and of the COUNCIL of 26 February 2014 on Public Procurement and Repealing Directive 2004/18/EC**

*Article 2 § 1*

(4) 'bodies governed by public law' means bodies that have all of the following characteristics:

- (a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;
- (b) they have legal personality; and
- (c) they are financed, for the most part, by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law;

**DIRECTIVE 2014/25/EU of the EUROPEAN PARLIAMENT and of the COUNCIL of 26 February 2014 on Procurement by Entities Operating in the Water, Energy, Transport and Postal Services Sectors and Repealing Directive 2004/17/EC**

*Article 3 § 4*

4. 'Bodies governed by public law' means bodies that have all of the following characteristics:

- (a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;
- (b) they have legal personality; and
- (c) they are financed, for the most part, by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or which have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law.

# General principles

## Article 44

### 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.**

*See also W(102)-W(102)*

Analysis	
Only condition:	<b>only if</b>
Subjective scope:	<b>controller and processor</b>
Objective scope:	<b>compliance with conditions</b>
Purposes:	<b>Ensuring the level of protection</b>

# Conditions for transfer under the GDPR

1. Adequacy decision
2. Transfers subject to appropriate safeguards
3. Binding corporate rules (BCR)
4. Derogations for specific situations

# The adequacy decision

# Adequacy decisions

European Commission website

[Adequacy of the protection of personal data in non-EU countries](#)

# Adequacy decisions - Article 45

<p><b>The first phase (evaluation) Article 45(1)(2)</b></p>	<p><b>Authority - 45(1)</b> European Commission</p>	<p><b>Judgement - 45(1)</b> Unquestionable of the European Commission</p>	<p><b>Subject of judgment - 45(1)</b> Ensuring an adequate level of protection</p>	<p><b>Assessment elements - 45(2)</b> a) the rule of law b) the existence and effective functioning of one or more independent supervisory authorities c) the international commitments</p>
<p><b>The second phase (implementing act) Article 45(3)</b></p>	<p><b>Duration (of the i. a.):</b> Temporary of 4 years (periodic review)</p>	<p><b>Content (of the i.a.):</b> Geographical and sectoral scope and, where possible, identify the supervisory authority or</p>	<p><b>Procedure (for adopting the i.a.):</b> Committee procedure - art. 93(2)</p>	
<p><b>The third phase (control) Article 45(4)</b></p>	<p><b>Powers of the Commission:</b> Monitoring on an ongoing basis</p>	<p><b>Scope of control:</b> Decisions taken under § 3 and Art. 25, § 6 of Directive 95/46/EC</p>		
<p><b>The fourth phase (control outcome) Article 45(5)(6)(7)</b></p>	<p><b>Possible outcome of the review:</b> Revocation, modification or suspension of the adequacy decision without retroactive effect (without prejudice to transfers under § 7)</p>			
<p><b>The fifth phase (Legal publication) Article 45(8)</b></p>	<p><b>Legal publication:</b> Official Journal of the European Union and EU Commission website.</p>			

**Previous decisions  
Article 45(9)**

**Decisions under  
Directive 95/46/EC:**  
In force until  
amended, replaced  
or repealed.

**See also:**

- *W(103)*
- *W(107)*
- *W(167)-(169)*

# Transfers EU-USA-EU

# Transfers EU-USA - Safe Harbour

## Once upon a time the “Safe Harbour”

CGEU - **JUDGMENT OF THE COURT (Grand Chamber) 6 October 2015** in Case C-362/14, REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings Maximilian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd,

On those grounds, the Court (Grand Chamber) hereby rules:

1. Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, **must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.**
2. **Decision 2000/520 is invalid.**

## Once upon a time the “Privacy Shield”

### COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield

#### From the European Commission website

The EU-U.S. Privacy Shield is based on the following principles:

- **Strong obligations on companies handling data:** under the new arrangement, the U.S. Department of Commerce will conduct **regular updates and reviews** of participating companies, to ensure that companies follow the rules they submitted themselves to. If companies do not comply in practice they face sanctions and removal from the list. The tightening of conditions for the **onward transfers** of data to third parties will guarantee the same level of protection in case of a transfer from a Privacy Shield company.
- **Clear safeguards and transparency obligations on U.S. government access:** The **US has given the EU assurance** that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms. Everyone in the EU will, also for the first time, benefit from **redress mechanisms** in this area. The U.S. has ruled out indiscriminate mass surveillance on personal data transferred to the US under the EU-U.S. Privacy Shield arrangement. The Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible. It details the safeguards in place for the use of data under such exceptional circumstances. The U.S. Secretary of State has established a **redress possibility** in the area of national intelligence for Europeans through an **Ombudsperson mechanism** within the Department of State.
- **Effective protection of individual rights:** Any citizen who considers that their data has been misused under the Privacy Shield scheme will benefit from several accessible and affordable dispute resolution mechanisms. Ideally, the complaint will be resolved **by the company** itself; or **free of charge Alternative Dispute resolution (ADR)** solutions will be offered. Individuals **can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved**. If a case is not resolved by any of the other means, as a last resort there will be an **arbitration** mechanism. Redress possibility in the area of national security for EU citizens' will be handled by an **Ombudsperson** independent from the US intelligence services.
- **Annual joint review mechanism:** the mechanism will monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national security purposes. The European Commission and the U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information available and will issue a public report to the European Parliament and the Council.

# What was happening in 2018 ....

JUDGMENT OF THE COURT (Third Chamber) 25 January 2018, in Case C-498/16, REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 20 July 2016, received at the Court on 19 September 2016, in the proceedings Maximilian Schrems v Facebook Ireland Limited,

## Document instituting the proceedings

“Mr Schrems brought an action before the Landesgericht für Zivilrechtssachen Wien (Regional Civil Court, Vienna, Austria), seeking, first, comprehensive declarations of the status of the defendant in the main proceedings as a mere service provider and of its duty to comply with instructions or of its status as an employer, where the processing of data is carried out for its own purposes, **the invalidity of contract terms** relating to conditions of use, second, an injunction prohibiting the use of his data for its own purposes or for those of third parties, third, disclosure concerning the use of his data and, fourth, the production of accounts and damages in respect of the variation of contract terms, harm suffered and unjustified enrichment.”.

There was a risk that standard contract clauses would also be declared invalid.

# Shrems II Judgement

Judgment of the Court (Grand Chamber) of 16 July 2020 in Case C-311/18 - REQUEST for a preliminary ruling under Article 267 TFEU from the High Court of Ireland made by decision of 4 May 2018, received at the Court on 9 May 2018, in the proceedings

**Referring court:** High Court (Ireland)

**Parties to the main proceedings:**

*Applicant:* Data Protection Commissioner

*Defendants:* Facebook Ireland Ltd, Maximillian Schrems

*Intervening parties:* The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance Inc., Digitaleurope

...

2. Article 46(1) and Article 46(2)(c) of Regulation 2016/679 **must be interpreted** as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. **To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.**
3. Article 58(2)(f) and (j) of Regulation 2016/679 **must be interpreted** as meaning that, unless there is a valid European Commission adequacy decision, **the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission**, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the Charter of Fundamental Rights, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.
4. Examination of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EU of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights **has disclosed nothing to affect the validity of that decision.**
5. **Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid.**

# The EDPB position



[European Data Protection Board publishes FAQ document on CJEU judgment C-311/18 \(Schrems II\)](#)

12 Questions and Answers

**Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems***

**Adopted on 23 July 2020**

1. <https://www.privacyshield.gov/welcome>
2. <https://www.privacyshield.gov/Program-Overview>



Search



Log In

Self-Certify

Privacy Shield List

Audiences

About

## WELCOME TO THE PRIVACY SHIELD

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

Please click on "Learn More" to read an important advisory regarding the status of the Privacy Shield Frameworks.

LEARN MORE



OCTOBER 07, 2022

# FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework



[BRIEFING ROOM](#) [STATEMENTS AND RELEASES](#)

Today, President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (E.O.) directing the steps that the United States will take to implement the U.S. commitments under the European Union-U.S. Data Privacy Framework (EU-U.S. DPF) [announced](#) by President Biden and European Commission President von der Leyen in March of 2022.

# Opinion of the Board (Art. 70.1.s)



**Opinion 5/2023 on the European Commission Draft  
Implementing Decision on the adequate protection of  
personal data under the EU-US Data Privacy Framework**

**Adopted on 28 February 2023**

Press release - 28/2/2023

**EDPB welcomes improvements  
under the EU-U.S. Data Privacy  
Framework, but concerns remain**



Home > Streaming > Committee on Civil Liberties, Justice and Home Affairs

2023-03-01 • 10:50 - 12:23  
**Committee on Civil Liberties, Justice and Home Affairs**  
Committee on Civil Liberties, Justice and Home Affairs

# Transfers subject to appropriate safeguards

# Transfers subject to appropriate safeguards

<p><b>Conditions Article 46(1)</b></p>	<p><b>Prerequisites:</b> the absence of an adequacy decision</p>	<p><b>Transfer permissible:</b> only if adequate safeguards are in place and those affected have enforceable data subject rights and effective legal remedies.</p>				
<p><b>Solution 1: Adequate safeguards Article 46(2)</b></p>	<p>(a) A legally binding and enforceable instrument between public authorities or bodies;</p>	<p>(b) Binding corporate rules in accordance with Article 47;</p>	<p>(c) Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);</p>	<p>(d) Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);</p>	<p>(e) An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or</p>	<p>(f) An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.</p>
<p><b>Solution 2: Additional appropriate safeguards Article 46(3)*</b></p>	<p>(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or</p>	<p>(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.</p>				
<p><b>Consistency mechanism Article 46(4)</b></p>	<p>The supervisory authority shall apply the consistency mechanism referred to in Article 63</p>					

## Previous authorizations Article 46(5)

On the basis of Article 26(2) of Directive 95/46/EC: in force until amended, replaced or repealed, if necessary, by a Commission Decision

\* With the authorisation of the supervisory authority

See also:

- [W108](#)
- [W109](#)
- [W114](#)

# Standard Contractual Clauses - SCC

# Model clauses prior to the current ones

## Nomenclature

*Standard data protection clauses*

*Model Contractual Clauses*

*Model clauses*

### EU controller - non-EU or EEA controller

**COMMISSION DECISION of 15 June 2001** on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC

**COMMISSION DECISION of 27 December 2004** amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries

### EU controller - non-EU or EEA processor

**COMMISSION DECISION of 5 February 2010** on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

# Standard Contractual Clauses (SCC)

On 4 June 2021, the European Commission adopted the following:

1. [COMMISSION IMPLEMENTING DECISION \(EU\) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation \(EU\) 2016/679 of the European Parliament and of the Council](#)
2. [COMMISSION IMPLEMENTING DECISION \(EU\) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28\(7\) of Regulation \(EU\) 2016/679 of the European Parliament and of the Council and Article 29\(7\) of Regulation \(EU\) 2018/1725 of the European Parliament and of the Council](#)

Those decisions were published in the OJEU on 7/6/2021.

The first decision contains as an Annex the new Standard Contractual Clauses (SCC) as required by the GDPR - Art. 46(2)(c) - for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR). These new SCCs replace the three SCCs adopted under the previous Directive 95/46/EC. As of September 27, 2021, contracts incorporating the previous SCCs **can no longer be concluded**.

**Until December 27, 2022** (formerly Art. 4(4) - *grace period* of 18 months), controllers and processors may continue to rely on the previous SCCs for contracts concluded before September 27, 2021, provided that the processing operations covered by the contract remain unchanged.

# The SCC structure (Impl. Dec. 914/2021)

- ➔ General clauses (articles from 1 to 7);
- ➔ Specific clauses (identified by MODULES) to be used according to the type of report, namely:
  1. MODULE ONE: Transfer **controller** to **controller**
  2. MODULE TWO: Transfer **controller** to **processor**
  3. MODULE THREE: Transfer **processor** to **processor**
  4. MODULE FOUR: Transfer **processor** to **controller**

# SCC advantages

- ➔ single document;
- ➔ modular approach;
- ➔ possibility of accession by other parties (so-called “docking clause”);
- ➔ transparency for stakeholders who can request copies (Art. 8-9 ..).

# How some big "players" behave ...

# Google

## Google Privacy & Terms

Overview **Privacy Policy** Terms of Service Technologies FAQ

**Introduction**

Information Google collects

Why Google collects data

Your privacy controls

Sharing your information

Keeping your information secure

Exporting & deleting your information

Retaining your information

Compliance & cooperation with  
regulators

About this policy

Related privacy practices

**Data transfer frameworks**

Key terms

Partners

Updates

<https://policies.google.com/privacy?hl=en>



### GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.



Privacy Checkup

Looking to change your privacy settings?

[Take the Privacy Checkup](#)

<https://policies.google.com/privacy/frameworks?hl=en>

Effective February 10, 2022 | [Archived versions](#) | [Download PDF](#)

# Facebook (Meta) & Privacy Shield

<https://www.facebook.com/about/privacyshield>

## META PLATFORMS, INC. AND THE EU-U.S. and SWISS-U.S. PRIVACY SHIELD

Meta Platforms, Inc. ("Meta") has certified to the [EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework](#) (collectively, "Privacy Shield Frameworks") with the US Department of Commerce regarding the collection and processing of personal data from our advertisers, customers, or business partners in the European Union, the United Kingdom, and, where a Swiss data controller uses Meta as a data processor, Switzerland ("Partners"), in connection with the products and services described in the Scope section below and in our [certification](#), although Meta does not rely on the EU-U.S. Privacy Shield Framework for transfers of personal data in light of the judgment of the Court of Justice of the EU in Case C-311/18. To learn more about the Privacy Shield programme, please visit [www.privacyshield.gov](http://www.privacyshield.gov).

**Scope:** Meta adheres to the Privacy Shield Principles (as set out in each of the Privacy Shield Frameworks) for the following areas of our business (collectively the "Partner Services"):

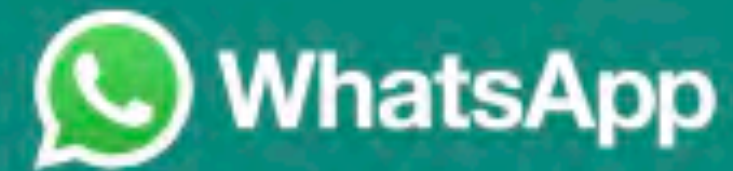
- **Workplace:** Workplace is a service that allows people to more effectively collaborate and share information at work. Partners (employers or organisations – the data controllers) may submit personal information about their members to Meta, with Meta Platforms Ireland Limited as the processor and Meta Platforms, Inc. as a sub-processor. While Partners and their members decide what information to submit, it typically includes things such as business contacts, customer and employee information, employee-generated content and communications, and other information under the Partner's control. For more information, members may contact the Partner through which they hold a Workplace account and review Workplace's [privacy policy](#).
- **Ads and measurement:** Meta offers ads and measurement products, and through those services, Meta may receive personal data from unaffiliated Partners (the data controllers) where Meta Platforms Ireland Limited is the processor and Meta Platforms, Inc. is a sub-processor. This includes things such as contact information and information about individuals' experiences or interactions with the Partners and their products, services and ads. For more information about our ads and measurement products, visit our [About Facebook Ads](#) page and our [Data Policy](#).

Meta uses the personal data provided by our Partners to provide Partner Services in accordance with the terms applicable to the relevant Partner Service and otherwise with the Partners' instructions.

[https://www.facebook.com/privacy/policy/?entry\\_point=data\\_policy\\_redirect&entry=0](https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0)

The screenshot shows the Facebook Privacy Centre interface. On the left, there is a navigation menu with the following items: 'Privacy Centre home', 'Privacy Policy' (which is highlighted with an upward arrow), 'What is the Privacy Policy and what does it cover?', 'What information do we collect?', and 'How do we use your information?'. The main content area on the right is titled 'Privacy Policy' and contains the following text: 'What is the Privacy Policy and what does it cover?' followed by 'Effective from 26 July 2022 | [View printable version](#)'. Below this, it states: 'We at Meta want you to understand what information we collect, and how we use and share it. That's why we encourage you to read our Privacy Policy. This helps you use Meta Products in the way that's right for you.' The next paragraph reads: 'In the Privacy Policy, we explain how we collect, use, share, retain and transfer information. We also let you know your rights. Each section of the Policy includes helpful examples and simpler language to make our practices easier to understand. We've also added links to resources where you can learn more about the privacy topics that interest you.' The following paragraph says: 'It's important to us that you know how to control your privacy, so we also show you where you can manage your information in the settings of the Meta Products you use. You can [update these settings](#) to shape your experience.' The final line in the screenshot says: 'Read the full policy below.'

# Whatsapp



WHATSAPP WEB

FEATURES

DOWNLOAD

PRIVACY

HELP CENTER

EN ▾

Last modified: January 04, 2021 ([archived versions](#))

## WhatsApp Privacy Policy

*If you live in the [European Region](#), WhatsApp Ireland Limited provides the services to you under this [Terms of Service](#) and [Privacy Policy](#).*

<https://www.whatsapp.com/legal/privacy-policy>

## Amazon.com Privacy Notice

1

Last updated: June 29, 2022. To see prior version, click [here](#).

We know that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This Privacy Notice describes how Amazon.com and its affiliates (collectively "Amazon") collect and process your personal information through Amazon websites, devices, products, services, online and physical stores, and applications that reference this Privacy Notice (together "Amazon Services"). **By using Amazon Services, you are consenting to the practices described in this Privacy Notice.**

- [What Personal Information About Customers Does Amazon Collect?](#)
- [For What Purposes Does Amazon Use Your Personal Information?](#)
- [What About Cookies and Other Identifiers?](#)
- [Does Amazon Share Your Personal Information?](#)
- [How Secure Is Information About Me?](#)
- [What About Advertising?](#)
- [What Information Can I Access?](#)
- [What Choices Do I Have?](#)
- [Are Children Allowed to Use Amazon Services?](#)
- [EU-US and Swiss-US Privacy Shield](#) ←
- [California Consumer Privacy Act](#)
- [Conditions of Use, Notices, and Revisions](#)
- [Related Practices and Information](#)
- [Examples of Information Collected](#)

## EU-US and Swiss-US Privacy Shield

2

Amazon.com, Inc. participates in the EU-US and Swiss-US Privacy Shield frameworks. Click [here](#) to learn more.

# Amazon

## EU-US and Swiss-US Privacy Shield

3

### EU-US Privacy Shield Framework

*We do not rely on the Privacy Shield but continue to keep to the commitments below that we made when we certified to the Privacy Shield.*

Amazon.com, Inc. and certain of its controlled US affiliates (together, the Amazon Group Companies, or "We") participate in the EU-US and Swiss-US Privacy Shield Framework regarding the collection, use, and retention of personal information from European Union member countries, the United Kingdom and Switzerland. We have certified with the Department of Commerce that we adhere to the Privacy Shield Principles. To learn more about the Privacy Shield Principles, visit [here](#). ←

If you have any inquiries or complaints about our handling of your personal information under Privacy Shield, or about our privacy practices generally, please contact us at: [privacysield@amazon.com](mailto:privacysield@amazon.com). We will respond to your inquiry promptly. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at: <https://www.verasafe.com/public-resources/dispute-resolution/submit-dispute/>. If neither Amazon nor our third-party dispute resolution provider resolves your complaint, you may pursue binding arbitration through the Privacy Shield Panel. To learn more about the Privacy Shield Panel, visit [here](#).

As explained [here](#) and [here](#) we sometimes provide personal information to third parties to perform services on our behalf. If we transfer personal information received under the Privacy Shield to a third party, the third party's access, use, and disclosure of the personal information must also be in compliance with our Privacy Shield obligations, and we will remain liable under the Privacy Shield for any failure to do so by the third party unless we prove we are not responsible for the event giving rise to the damage. ←

You can review our Privacy Shield registration [here](#). The Amazon Group Companies are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). We may be required to disclose personal information that we handle under the Privacy Shield in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

<https://www.amazon.com/gp/help/customer/display.html%3FnodeId%3DGX7NJQ4ZB8MHFRNJ>



<https://www.apple.com/legal/privacy/en-ww/>

# Apple Privacy Policy

Updated October 27, 2021

Apple's Privacy Policy describes how Apple collects, uses, and shares your personal data.

In addition to this Privacy Policy, we provide data and privacy information embedded in our products and certain features that ask to use your personal information. This product-specific information is accompanied by our Data & Privacy Icon.



You will be given an opportunity to review this product-specific information before using these features. You also can view this information at any time, either in settings related to those features and/or online at [apple.com/legal/privacy/data](https://apple.com/legal/privacy/data).

Please take a moment to familiarize yourself with our privacy practices, accessible via the headings below, and [contact us](#) if you have any questions.

[Download a copy of this Privacy Policy \(PDF\)](#)

[Your California Privacy Disclosures >](#)

[Information Regarding Commercial Electronic Messages in Canada >](#)

[Apple Health Study Apps Privacy Policy >](#)

## Transfer of Personal Data Between Countries

Personal data relating to individuals in the European Economic Area, the United Kingdom, and Switzerland is controlled by Apple Distribution International Limited in Ireland. Apple's international transfer of personal data collected in the European Economic Area, the United Kingdom, and Switzerland is governed by [Standard Contractual Clauses](#). Apple's international transfer of personal data collected in participating Asia-Pacific Economic Cooperation (APEC) countries abides by the [APEC Cross-Border Privacy Rules \(CBPR\) System](#) and [Privacy Recognition for Processors \(PRP\) System](#) for the transfer of personal data. If you have questions or unresolved concerns about our APEC CBPR or PRP certifications, contact our [third-party dispute resolution provider](#).



# Binding Corporate Rules (BCR)

# BCR - Definitions

## Article 4(20)

**'binding corporate rules'** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

## Article 4(19)

**'group of undertakings'** means a controlling undertaking and its controlled undertakings;

# BCR - Schema

<p><b>Procedure</b> <b>Article 47(1)</b></p>	<p><b>Authority:</b> The competent supervisory authority (Lead Authority)</p>	<p><b>Criterion:</b> Consistency mechanism set out in Article 63</p>	
<p><b>Conditions</b> <b>Article 47(1)</b></p>	<p>(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their</p>	<p>(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and</p>	<p>(c) fulfil the requirements laid down in paragraph 2.</p>
<p><b>Content of the BCRs</b> <b>Article 47(2)</b></p>	<p>The binding corporate rules referred to in paragraph 1 shall specify at least: ... From letter (a) to letter (n)</p>		
<p><b>Commission's Role</b> <b>Article 47(3)</b></p>	<p>The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).</p>		

**See also:**

- *W110*
- *W167-168*

# Summary of the procedure for BCRs

1. The "Group" (**applicant**) submits documentation for BCRs and:
2. Identifies the SA "Lead Authority";
3. The cooperation procedure for approval of BCRs is initiated:
  - 3.1. The SA identified as the LA:
    - a) informs the other SAs involved indicating whether or not it agrees to be the LA;
    - b) invites the other SAs to raise any objections within two weeks (period extendable to another two weeks if requested by any interested SA);
    - c) silence is considered as assent;
    - d) Suppose the SA identified as the LA believes it should not act as the lead authority. In that case, it should explain its decision and recommendations (if any) on which other SA would be the appropriate lead authority.
4. Having completed the phase on the identification of the LA, **the discussion with the applicant is opened**;
5. A first draft is sent to one or two SAs involved who serve as co-reviewers and must send any comments within one month (if not, silence counts as assent);
6. Upon completion, there will be a "consolidated draft" that the applicant/applicant must send to the other SAs involved for comments, which must be received no later than one month;
7. If there are comments, a new discussion will be opened with the applicant/applicant;
8. If no comments are received from the other SAs, the text is deemed approved;
9. The LA will send the "final draft" with any accompanying documentation to the EDPB, who will decide according to the rules of procedure.

# Template for the BCR

*Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data*

**WP265**

**Adopted on 11 April 2018**  
**Endorsed by the EDPB on 25/5/2018**

## Standard Application for Approval of Binding Corporate Rules for Processors

### PART 1: APPLICANT INFORMATION

#### 1. STRUCTURE AND CONTACT DETAILS OF THE GROUP OF UNDERTAKINGS OR GROUP OF ENTERPRISES ENGAGED IN A JOINT ECONOMIC ACTIVITY (THE GROUP)

Name of the Group and location of its headquarters (ultimate parent company):  
[REDACTED]

Does the Group have its headquarters in the EEA?

Yes  
 No

Name and location of the applicant:  
[REDACTED]

Identification number (if any): [REDACTED]

Legal nature of the applicant (corporation, partnership, etc.):  
[REDACTED]

Description of position of the applicant within the Group:

(e.g. headquarters of the Group in the EEA, or, if the Group does not have its headquarters in the EEA, the member of the Group inside the EEA with delegated data protection responsibilities)  
[REDACTED]

Name and/or function of contact person (note: the contact person may change, you may indicate a function rather than the name of a specific person):  
[REDACTED]

Address:  
[REDACTED]

Country:

Phone number: [REDACTED]

Fax: [REDACTED]

E-Mail: [REDACTED]

EEA Member States from which BCRs for Processors will be used:  
[REDACTED]

# Approved BCR

**Approved BCR by the EDPB -> [on the institutional EDPB website](#)**

A list of **pre-GDPR** BCR approved before 25 May 2018 -> [on the EDPB website](#)

**Approved BCR adopted **pre-GDPR** by the Garante -> [on the institutional website](#)**

# Derogations for specific situations

# Derogations for specific situations

## Prerequisites - art. 49(1)

In the absence of an adequacy decision, appropriate safeguards, or BCRs

## Conditions - art. 49(1)

- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation **may take place only** if the transfer is not repetitive, concerns only a limited number of data subjects is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued. ([see par. 2.8 of the EDPB Guidelines 2/2018](#)).

*See also: W111-114*

# Thank you for your attention!

**Nicola Fabiano**

<https://bio.link/nicfab>



@nicfab



**LinkedIn**



@nicfab@nicfab.it



[Privacy Community](#)



[NicFab Channel](#)