

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

Principles relating to processing of personal data

Cristina Radu

Palermo, 19 May 2023



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



INTRODUCTION

Prior protection of personal data

Art. 8 of ECHR (European Convention on Human Rights) 1950:

”Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”



INTRODUCTION

September 1980 - OECD (the Organization for Economic Cooperation and Development) issued a set of guides for data protection - *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* establishing some main principles:

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.



INTRODUCTION

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.



INTRODUCTION

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;



INTRODUCTION

- b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8.Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

The OECD guidelines obtained the status of global standard but with a limited effect for member states - non - binding



INTRODUCTION

➤ 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*

“PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

- (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;



INTRODUCTION

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.'

These principles fall into three categories: transparency, legitimate purpose and proportionality.



- the **Regulation (EU) 2016/679** of the European Parliament and of the Council *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 (GDPR)* adopted on 27th of April 2016.

Article 5 - Principles relating to processing of personal data

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability



Comparison between the Directive and the GDPR

Generally, the principles were part also of the Directive, with new additions now within the GDPR, for example the exception of the archiving purposes in the public interest, conditions and guarantees for longer periods storage of the data and the most important, the accountability principle.

Directive :

2. It shall be for the controller to ensure that paragraph 1 is complied with.'

GDPR

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

As per Cambridge English Dictionary: "Someone who is accountable is completely responsible for what they do and must be able to give a satisfactory reason for it"



The principles relating to processing of personal data are the heart/center of the GDPR. They are presented at the beginning of the regulation and represent the basis of all the further clauses. The principles do not establish demanding provisions, but incorporate the spirit of the general regime in what concerns the data processing.

Importance: the principles determine, in a general manner, the conditions under which an entity can process personal data.

Sanctions: up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher for non-compliance with the principles relating to the processing of personal data

1. Lawfulness, fairness and transparency

Article 5 par 1 letter (a) *Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')*

Lawfulness

- Necessary to Identify specific legitimate grounds for processing, presented as “lawfulness for processing” - Article 6 GDPR - there are 6 options depending on the controller purposes and the relation with the data subject. Also, there are additional conditions for processing sensible data. If no legal ground for processing is given, the processing is illegitimate and in breach of this principle. Breach of lawfulness also if the processing does not observe a legal obligation, an agreement, legislation or human rights
- Articles 6 - 10 GDPR

Fairness

- The controller should process data only in a manner reasonable for the data subjects and not to use the data in manners with negative effects on them. If a person is deceived with the purpose of obtaining their personal data - the processing is not fair. Fair reaction of the controller when the data subjects exercise their rights granted by the GDPR





1. Lawfulness, fairness and transparency

Transparency

- A milestone for the GDPR
- Under the Directive the right to information ensured a fair processing towards the data subjects. Now, the transparency is imposed in all situations of processing, from the collecting data till a proper handling of requests for exercising their rights. New also: obligation of data controllers to notify data security breach to the data subjects involved
- The controller shall inform the data subject completely, correctly and objectively prior to processing their data or in any further change regarding the collected data and the processing.
- Articles 13-14 GDPR
- Novelty of the GDPR - obligation for data controller to clearly and specifically inform the data subjects not only when they obtain the data directly from the subjects, but also from third parties.
- Transparency= premise for the observance of data subjects fundamental rights.



2. Purpose limitation

Article 5 par 1 letter (b) *Personal data shall be: (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')*

- Related to the lawfulness, fairness and transparency principle
- The personal data must be used only in the purpose for which they were collected and if the processing for a new purpose is necessary, the data subject needs to be informed and, if the case, needs to offer the consent for this new processing and purpose, observing thus also the transparency principle
- Not a novelty but the GDPR brings the interdiction to use data (initially collected for a purpose) for new purposes incompatible with the former without the notice and consent of the data subject (ex. Data for marketing used for profiling)
- The controller must analyze the purposes for processing in relation to the legal grounds for processing, to inform the data subject and to obtain their consent, if necessary for the new purposes



2. Purpose limitation

- The controller must determine the purposes-if the obligations regarding the documentation and transparency are observed, there are high chances to observe also the obligation to determine and specify the purposes. The purpose must be presented within the documentation kept as an obligation on the evidence of the processing operation and also be presented within the privacy notice for the data subject. The data subject must be informed on the purpose of processing their personal data. Note: not any description of the purpose or informing on such transform an illegitimate processing into a legitimate one
- The GDPR does not forbid the use of the personal data for another purpose compatible with the initial one as long as the subject is informed and if a consent was given, to obtain their new consent
- what is an incompatible purpose? In order to determine this it needs to be analyzed the relation between the initial and new purpose, the nature of the personal data, the consequences of this new processing and if there are adequate guarantees (pseudonymisation) (ex. A doctor discloses his patients list to his daughter, who owns a travel agency for the latter to send them travel offers for spa recovery treatment)



3. Data minimization

Article 5 par 1 letter (c) *Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

- A novelty principle - GDPR brought the obligation for a controller to establish the minimum level of personal data strictly needed for their activity. Before the GDPR- it was used the term *non-excessive data* but now there is an express obligation for the minimum data.
- The controller must analyze what personal data is processing and if those are not anymore necessary for its activity, to limit them by erasing the data processed with no clear, legal and grounded purpose
- First step - to analyze the purpose of processing and the quantity of data necessary for such purpose. The minimum of data is a request. For example, for commercial emails there is no necessity for the ID data of the subject.
- All the additional collected data must be erased
- No personal data more than the minimum necessary ones could be collected and thus, processed for observing the data minimization purpose



4. Accuracy

Article 5 par 1 letter (d) *Personal data shall be: (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').*

- Not a novelty also, but the GDPR brings the obligation of updating the personal data if necessary (ex. Change of name, address, phone number)
- Obligation for data controller to ensure that the processed data are accurate and the ones inaccurate to be updated/rectified or deleted
- The controller must check the modality to communicate with the data subject (e-mail, phone etc) and to use this for updating the data. If the person cannot be reached, those personal data must be erased.
- Processes and procedures must be prepared by the controllers in order to ensure the accuracy of the data and their update, from time to time
- A novelty related to this principle is *the right to be forgotten (article 17)* - the right of the data subject to obtain the erasure of their personal data concerning him or her without undue delay when the personal data are no longer



4. Accuracy

necessary in relation to the purposes for which they were collected or the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing or the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the personal data have been unlawfully processed.

- The controller must take reasonable measures to ensure that the personal data are accurate and otherwise, the inaccurate data are erased or rectified without undue delay
- The controller shall ensure the correction, the supplementation, update or the erasure of the inaccurate or incomplete personal data.



5. Storage limitation

Article 5 par 1 letter (e) *Personal data shall be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').*

Rule - the personal data shall be kept only for the time necessary for the purposes of processing

Exception - the personal data may be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

The storage of the data for periods incompatible with the processing purposes might attire losses for the controller and deteriorations of the data and sanctions from the competent authority.

5. Storage limitation

The controllers need to take special measures, to implement operational processes and data retention procedures for a good evidence of the modality and place of storage, the erasure procedure and the anonymization of the personal data which need not to be processed anymore. This process implies also the interdiction for the controller employees to copy the data on local devices or mobile devices (USB)

As a request for the controllers in relation to this principle is their obligation to inform their processors on the retention period and related instructions to erase or return the data at the end of the processing.

Some personal data cannot be erased at the decision of the controller, but observing some legal mandatory terms, ex. fiscal documents need to be kept for a longer period, as a legal obligation.

From the moment the data are not necessary for the processing purpose, these need to be either subject to anonymization or to erasure.





6. Integrity and confidentiality

Article 5 par 1 letter (f) *Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

The milestone of the GDPR - the controllers must ensure the protection of the personal data against external risks (cyber attacks) as well as internal risks (accidental losses, accidental erasure)

The novelty is that the GDPR transforms the integrity and confidentiality into a principle, not only an obligation as per the Data Protection Directive.

The controllers are obliged to take, according to their possibilities, technical and operational measures proportional with the risks and rights of the data subjects - ex. anonymisation, encryption. The technical implementation is not sufficient, as long as the organizational procedures are not taken into consideration. For example, in Romania, the Data Protection Authority has sanctioned with a significant fine an important bank due to the unauthorized disclosure of a client personal data by one of its employees on social media.



6. Integrity and confidentiality

The controllers need to take internal measures, to properly instruct their employees, as part of the GDPR obligations and in order to ensure the observance of the integrity and confidentiality principle. In practice, for example are implemented confidentiality agreements with the employees, consultants and any other party with access to the personal data, there is usually inserted a restriction system of the access only based upon a safe password in order for the involved parties to access only the personal data necessary for their attributions.

It is necessary for the controllers to evaluate the data processing within their company, to ensure the operational data flow in a safe mode and according to every employees capabilities, to ensure the existence of clear security and data access policies, of adequate technical measures for preventing the unauthorized access and the possible data loss (ex. malware) and above all, to set a control system of the entire data processing.

In relation to this principle GDPR brings the obligation for the controller to inform with no delay the data protection authority (not later than 72 hours from the incident) and the data subjects in case of a data breach. It is acknowledged the importance of this principle, which stays at the base of the GDPR implementation.



7. Accountability

Article 5 par 2 *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

Based on the Directive the accountability was an implicit requirement of data protection law; currently, in the GDPR it has become a cornerstone of effective personal data protection. The principle ensures that throughout the processing, the controllers take responsibility for correspondingly observing all the principles of data protection, including the security and confidentiality of the personal data they process. The controllers need to implement adequate technical and organizational measures to guarantee and demonstrate that they comply with all the principles for data processing.

As per the Cambridge Dictionary - *accountability = the fact of being responsible for what you do and able to give a satisfactory reason for it, or the degree to which this happens; responsibility = something that it is your job or duty to deal with.*

According to the Working Group established as per article 29 of the GDPR this principle includes two elements: (i) the controller obligation to establish effective, necessary measures for compliance with the principles set in the GDPR and (ii) the controller obligation to demonstrate the fact that they had taken the adequate measures for data protection.



7. Accountability

(i) The controller must implement proper technical and organizational measures to ensure that the personal data are processed in accordance with the GDPR, taking into consideration the nature, field of application, context and processing purposes, the levels of the risk for the rights and freedoms of the data subjects (ex. Sensible data, children data etc). These measures need to be revised and updated from time to time. Practical measures presented by the GDPR for such obligation: ensuring the data protection starting with the moment of creation and implicitly - privacy by design and by default (art. 25); the evidence of the processing activities (art. 30); the evaluation of the impact over the data protection (art. 35); appointment of a data protection officer (art. 37-39) etc.

According to the opinion of the European Data Protection Board (EDPB) 4/2019 the technical and organizational measures can be considered as any measure or guarantee implementing the data protection principles, considering the context and the risks of processing. There are presented as effective measures: using of advanced technical solutions, basic instruction of the personnel, pseudonymisation of personal data, storage of the data in a structured format, currently used and that can be read automatically, detaining systems for tracing malware programs, implementing some management systems for confidentiality and information security, contractual clauses to oblige the processors to implement specific measures for minimization of data.

7. Accountability

Recital no. 78 of the GDPR: *in order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.*

In practice, there are implemented internal policies for: managing and supervising the compliance with the data protection regulations, the careful selection of the data processors, the ensuring of transparency, training courses for the employees, the permanent monitoring and procedures for dealing with the requests of data subjects



7. Accountability

(ii) Demonstrate the compliance

Recital no. 77 of the GDPR: *Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, **could be provided** in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer.*

The controller can demonstrate the compliance by keeping the documentation requested by the GDPR as: the evidence of processing activities (art. 29), *the registry for data breach (art. 30), DPIA Registry - Data Protection Impact Assessment (art.31).*

In practice, as part of the documentation are also: privacy notices on the processing of their personal data for the clients, employees, candidates; preparing internal policies on the data processing, inserting data protection clauses within the contracts concluded with third parties including guarantees for data protection and standard contractual clauses regarding the data transfers, evidence of the training courses for the employees



7. Accountability

In what regards the documentation and the measures, as per the GDPR, the data controllers must take into consideration the actual status of the technology, the costs for implementation and the nature, field of applying, context and purposes of processing, as well as the risks with different levels of probability and gravity for the rights and freedoms of the data subjects triggered by the processing.

The Romanian Data Protection Authority sanctioned the non-compliance with article 5 of the GDPR regarding the principles relating to processing of personal data in various cases, for example:

- in the banking field - sanctioned with Euro 5,000 the Romanian Commercial Bank for not implementing adequate measure to ensure that any employee acting under the bank authority acts only at the controller request. It was revealed a collection of identity cards copies of the clients through the personal phone of an employee of the controller, as well as the transfer of such copies through WhatsApp, with the violation of internal procedure.
- also, fined with Euro 130,000 Unicredit Bank for the insufficient adequate technical and organizational measures triggering the online disclosing of identity cards and addresses of thousands of data subjects, clients of the bank;



7. Accountability

- In the telecommunication field - a fine of Euro 25,000 for Telekom for not implementing adequate technical and organizational measures for ensuring a proper security level for the processing risk, which triggered the unauthorized disclosure and access to personal data of the clients as: client ID, client code, name and surname, personal identification number, place and date of birth, phone number for thousands of data subjects. The invoicing data have been wrongly inserted in the data base transferred to a contractual partner for assignment of receivables, being sent wrongful notifications to these persons
- In the transportation field -a fine of Euro 20,000 for TAROM after one of the employees has accessed (unauthorized) the booking application and made photos of a list of 22 passengers, disclosing the list afterwards online
- In 2021, a natural person was also sanctioned with Euro 500 for not implementing adequate technical and organizational measures triggering the disclosure to the public of personal data (surname, name, signature, citizenship, date of birth, address, series and number of the identity card and the political option) for 10 data subjects.



7. Accountability

Thus, to demonstrate the compliance with this new principle, the controllers must implement policies and procedures in accordance with GDPR, in order to ensure the observance of the data subjects rights and their personal data protection.

Shortly, the controllers shall analyze the following: if and how they process the personal data, which personal data are necessary for their activity, the purpose of such data, which is the modality of informing the data subjects, the protection of personal data. Based on these information, the controller must prepare the data flow and the processes for using the personal data, considering various specific facts, for example the complexity of processing and the volume of personal data.

For complying with the accountability principle - technical and organizational measures must be taken at the level of any organization, being implemented an advanced internal culture for data protection, being mandatory for all these measures to be verified and updated from time to time to ensure the safe processing of personal data.



CONCLUSION

All the principles relating to processing of personal data must be observed by the controllers and processors. The compliance with these principles is the background for good practices on data protection field, being essential for the compliance with all GDPR provisions. Moreover, the non-compliance with the principles triggers substantial fines, at the highest level of administrative fines.

The core of the principles is the one included expressly in the GDPR, the accountability principle which needs to be remembered with its two elements: the implementation of the technical and organizational measures and the demonstration of compliance.

In a very short list of measures for a controller to comply with the principles there might be included: the identification of legitimate grounds for collecting and processing of personal data, to ensure that the personal data are not used in breach of any other law, to process the data with fairness, not triggering a damage for the data subject, to offer all the information to the data subjects by being clear and open on the processing of their data and especially to take all adequate measures for protection of the data.





THANK YOU FOR YOUR ATTENTION!

GRAZIE PER L' ATTENZIONE!

Cristina Radu

Partner



Cristina.radu@monolit.ro

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

Data controller and data processor

Filippo Bianchini

Palermo, 19 May 2023



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

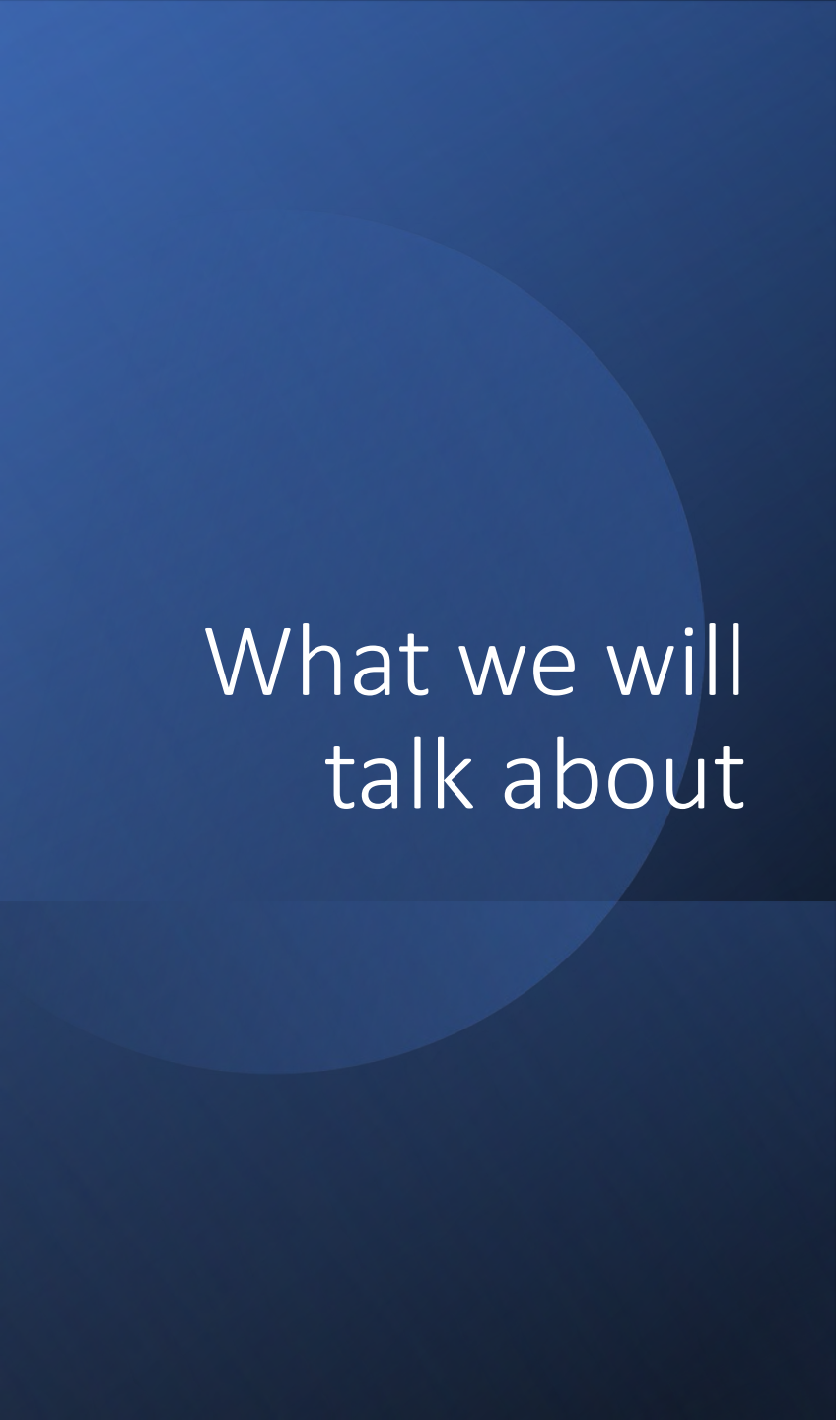
>_who I am

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

Privacy roles

ARTICLE 29 DATA PROTECTION WORKING PARTY



00264/10/EN
WP 169

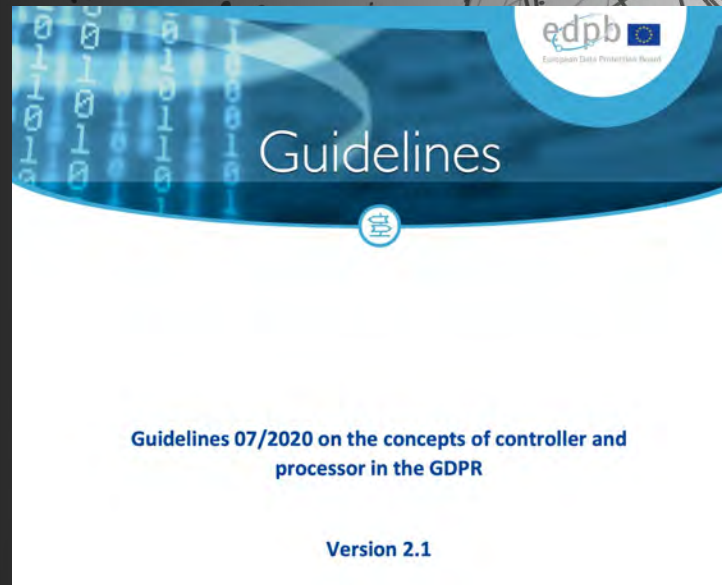
Opinion 1/2010 on the concepts of "controller" and "processor"

Adopted on 16 February 2010

Training of Lawyers on
EU Law relating to Data
Protection 2



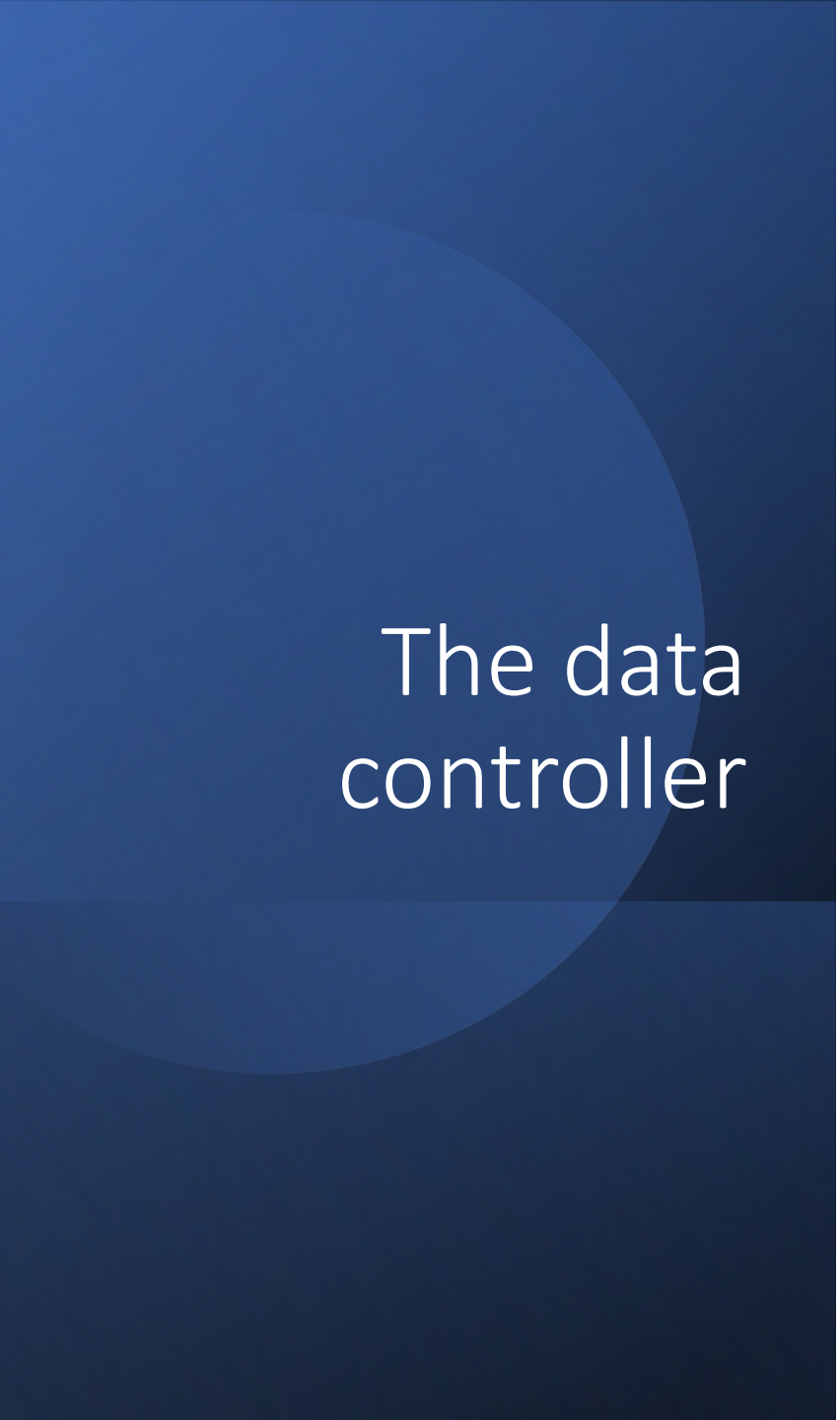
#TRADATA2



The data controller

Definition

Purposes of the processing



The data controller

The data processor

Definition

Processor vs. appointee

Companies providing payroll services

The joint controllers

Training of Lawyers on
EU Law relating to Data
Protection 2



Definition



Shared Purposes and Means



Facebook fan pages and use of Insight services



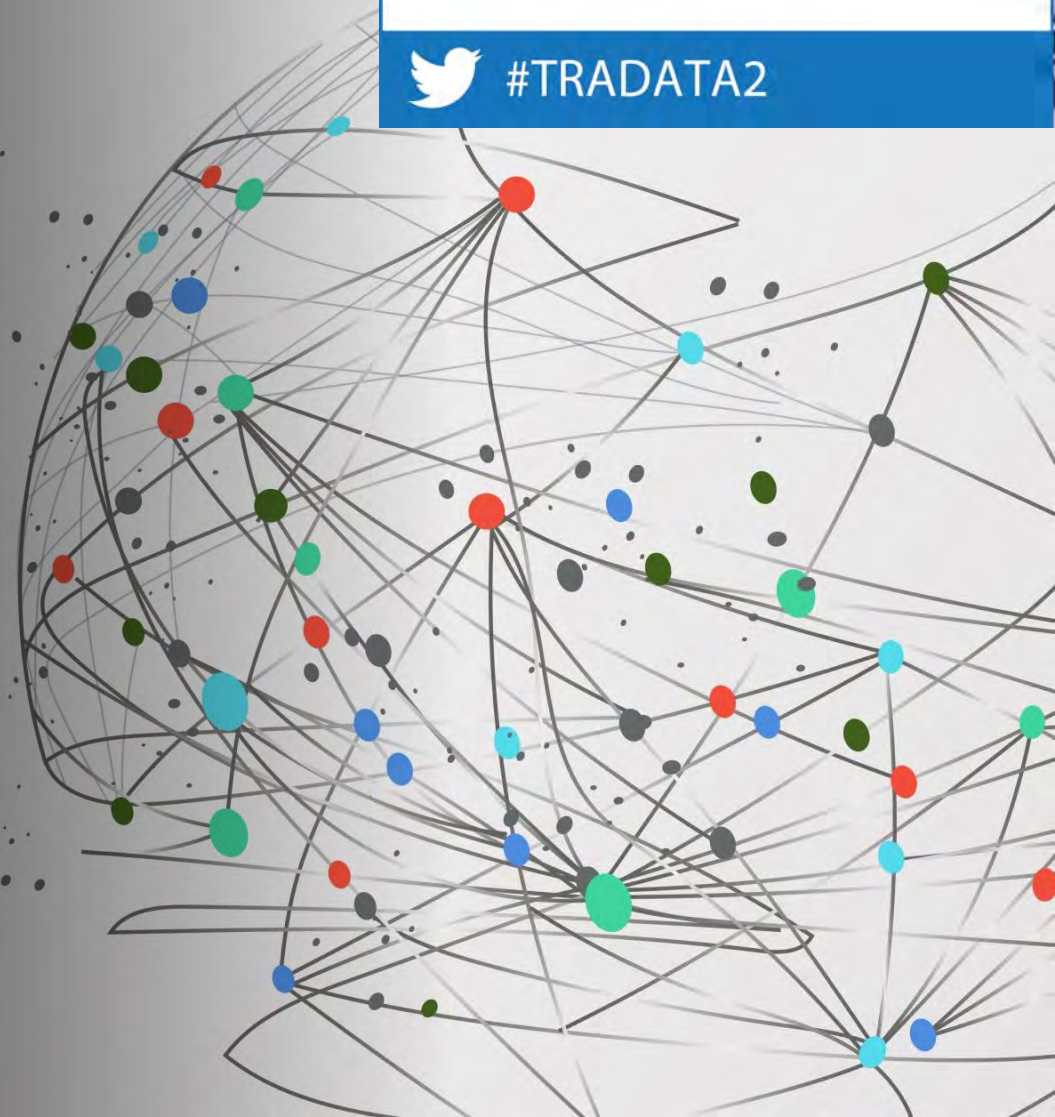
[The EDPB Guidelines on Social Media Targeting](#)



#TRADATA2



Obligations and liability



Regulatory
obligations

Obligations of the data controller

Responsibilities and their allocation

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Joint and several liability
(Art. 82)

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

Data Processing Agreements (DPA)

Preliminary verification

- Due diligence

Written authorisation

Minimum statutory content

Future
challenges

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Artificial Intelligence

Blockchain

Web3



Thank you for your attention!

Filippo Bianchini

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

LinkedIn: [studiolegale](#) – Twitter: [@legale](#)

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

**Rights of data subjects, including criminal
investigations and proceedings**

Giovanni Battista Gallus

Palermo, 19 May 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. Bardan, 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 & Partners



Who am I

- Lawyer - 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

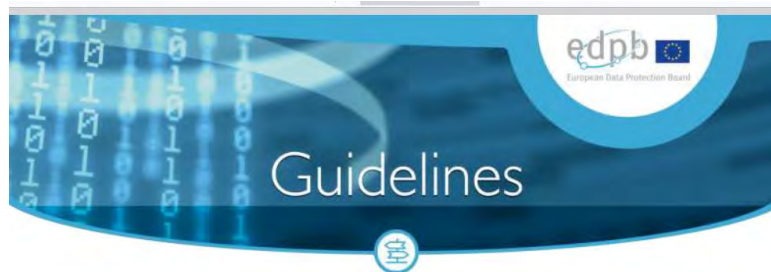
As last Revised and Adopted on 11 April 2018



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

Version 2.0

Adopted on 28 March 2023



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



#TRADATA2



Common principles

Data Subject rights - definitions

We all know the
definition of
Personal data...

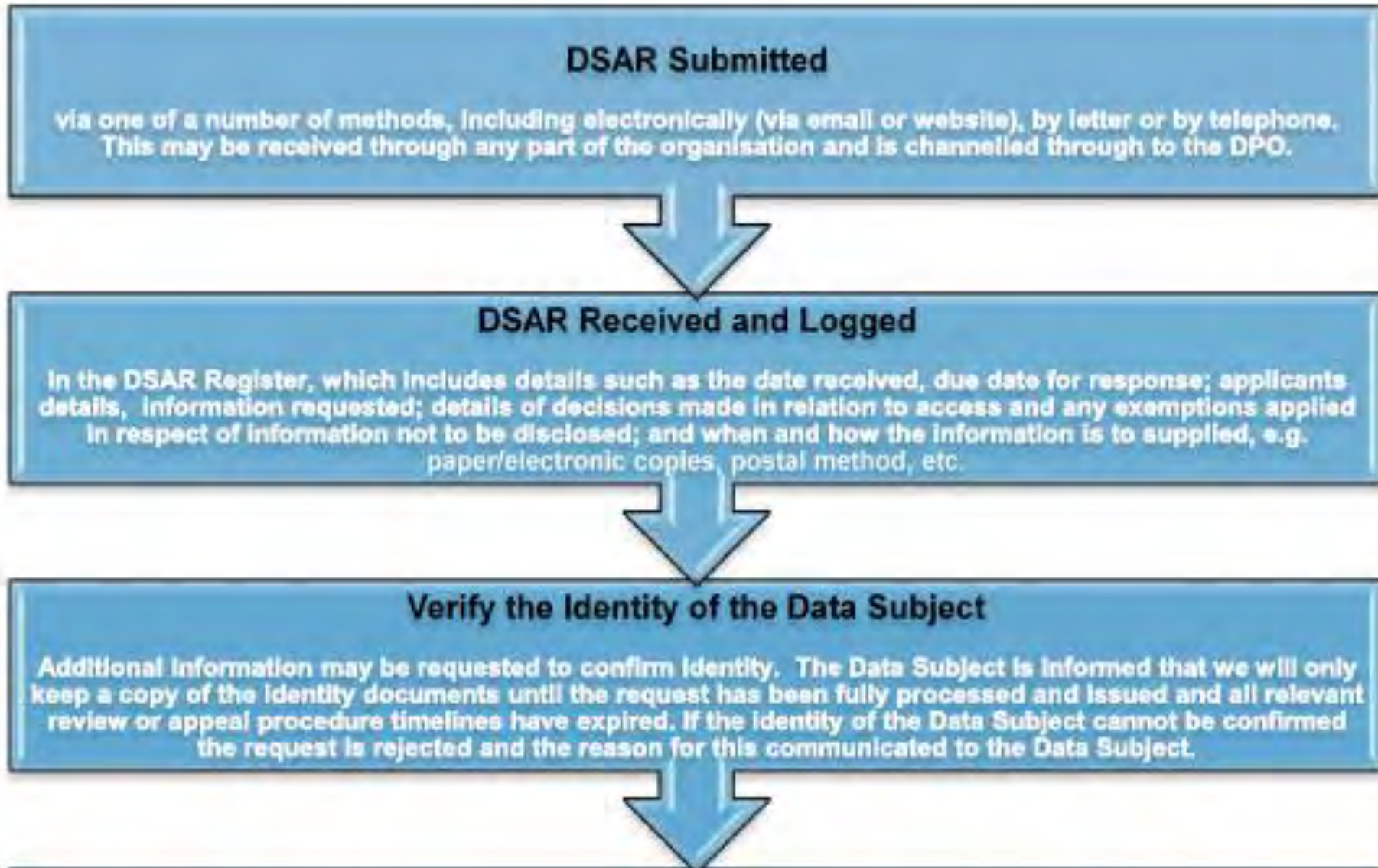


We all know
who the Data
subject is...

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

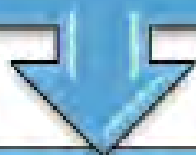
Version 1.0

Adopted on 18 January 2022



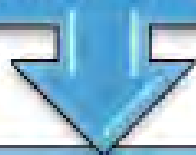
Evaluate Validity of Information Provided

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



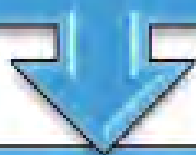
Identify and Compile the Personal Data

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

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

Oggetto

PROTEZIONE DATI
PERSONALI

Ud. 24/2/2023 CC

ha pronunciato la seguente

ORDINANZA

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

ER MODELLO ATE Serial# 26945c6a038cf32b
1857b4bedec31d59

A quick overview of the rights

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

EU	Issues covered	CoE
Right to be informed		
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)

Right of access

General Data Protection Regulation,
Article 15 (1)
CJEU, C-553/07, *College van
burgemeester en wethouders van*

Right of access to
one's own data

Modernised
Convention 108,
Article 9 (1) (b)
ECtHR, *Leander*

EU

Issues covered

CoE

CJEU, Joined cases C-141/12 and
C-372/12, *YS v. Minister voor
Immigratie, Integratie en Asiel and
Minister voor Immigratie, Integratie
en Asiel v. M and S*, 2014
CJEU, C-434/16, *Peter Nowak v. Data
Protection Commissioner*, 2017

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

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, <i>Cemalettin Canli v. Turkey</i> , No. 22427/04, 2008 ECtHR, <i>Ciubotaru v. Moldova</i> , 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, <i>Segerstedt-Wiberg and Others v. Sweden</i> , No. 62332/00, 2006
CJEU, C-131/12, <i>Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [GC], 2014 CJEU, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni</i> , 2017	The right to be forgotten	

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

Right to restriction of processing		
General Data Protection Regulation, Article 18 (1)	Right to restrict use of personal data	
General Data Protection Regulation, Article 19	Notification obligation	
Right to data portability		
General Data Protection Regulation, Article 20	Right to data portability	
Right to object		
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	
Rights related to automated decision-making and profiling		
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

Microsoft Ignite

October 12-14, 2022

[Register now >](#)

 **Microsoft** | [Learn](#) [Documentation](#) [Training](#) [Certifications](#) [Q&A](#) [Code Samples](#) [Shows](#) [Events](#)

[Sign in](#)

- > Microsoft compliance offerings
 - > General Data Protection Regulation (GDPR)
 - GDPR overview
 - Recommended action plan for GDPR
 - Deploy information protection for data privacy regulations
 - Microsoft's data protection officer
 - > Accountability readiness checklists
 - > Data subject requests
 - Data subject requests
 - Manage data subject requests with the DSR case tool
 - Azure
 - Azure DevOps services
 - Dynamics 365
 - Intune
 - Microsoft Support & Professional Services
 - Office 365**

[Learn](#) / [General Data Protection Regulation \(GDPR\)](#) / [Data subject requests](#) /

Office 365 Data Subject Requests for the GDPR and CCPA

Article • 09/27/2022 • 130 minutes to read • 5 contributors

Introduction to DSRs

The European Union [General Data Protection Regulation \(GDPR\)](#) ¹ 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.

In this article

- [Introduction to DSRs](#)
- [Part 1: Responding to DSRs for Customer Data](#)
- [Using the Content Search eDiscovery tool to respond to DSRs](#)
- [Providing a copy of personal data](#)

[Show more](#) ▾

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
- ...

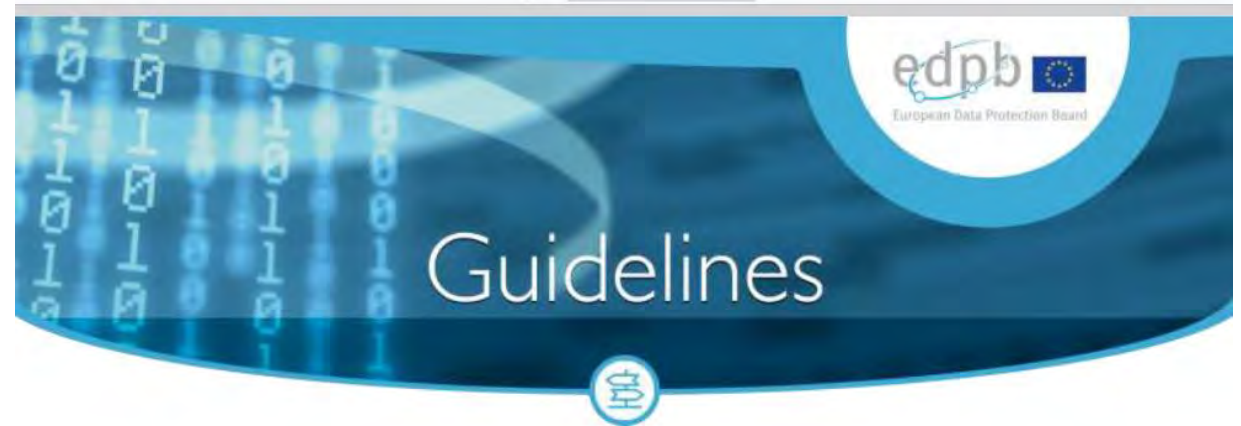
Focus on the right of
access

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 2.0

Adopted on 28 March 2023

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



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

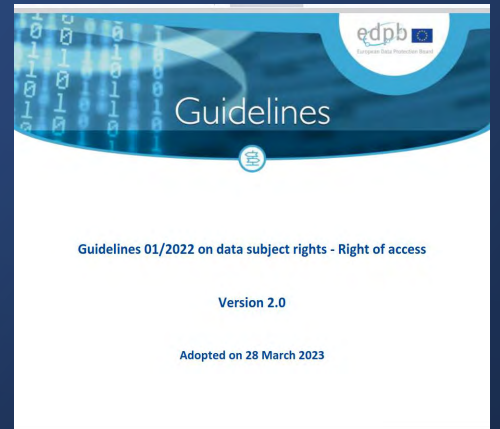
[September plenary - adopted documents](#)

 20 September 2022 EDPB

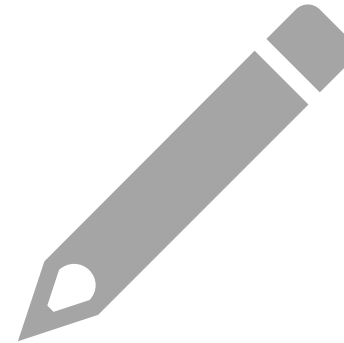
[New EDPB opinion on certification criteria](#)

Summary of the Decision

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.

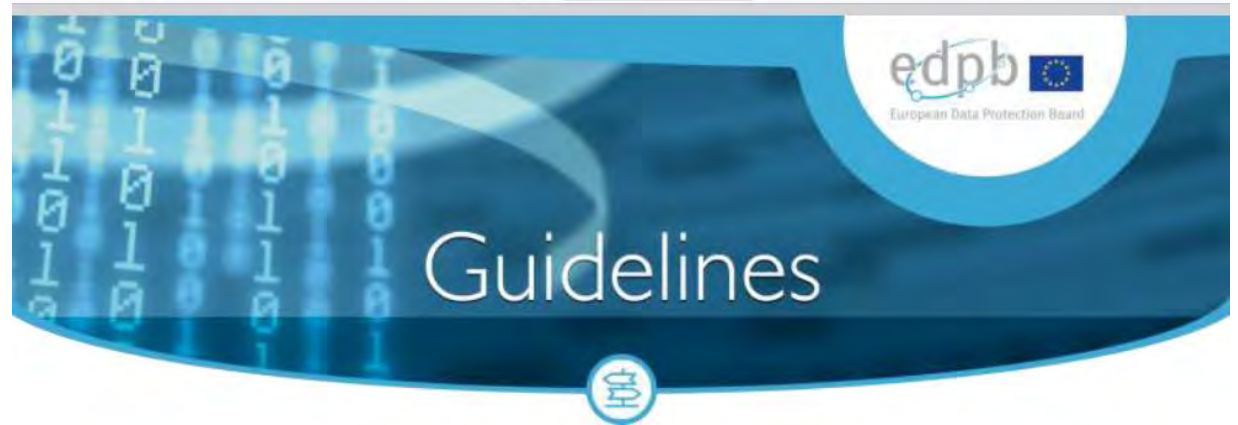
The right of access

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 2.0

Adopted on 28 March 2023



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

y

Does the data subject has 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

y

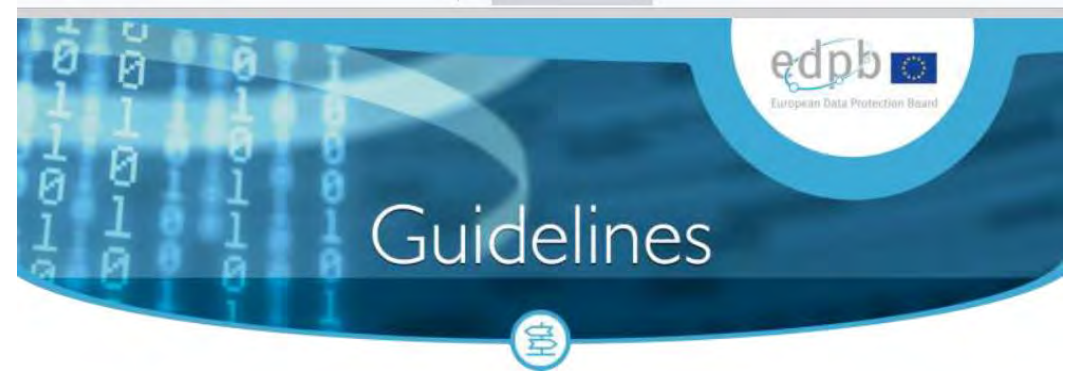
Does the data subject has the right to know the specific identity of the recipients?

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.



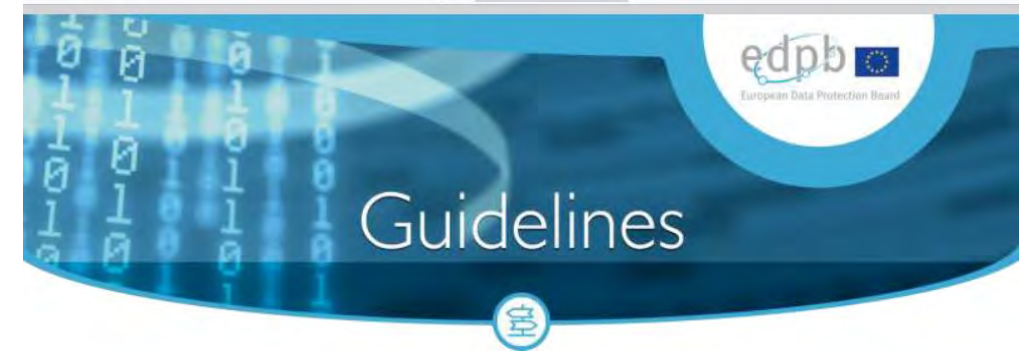
Guidelines 01/2022 on data subject rights - Right of access

Version 2.0

Adopted on 28 March 2023

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



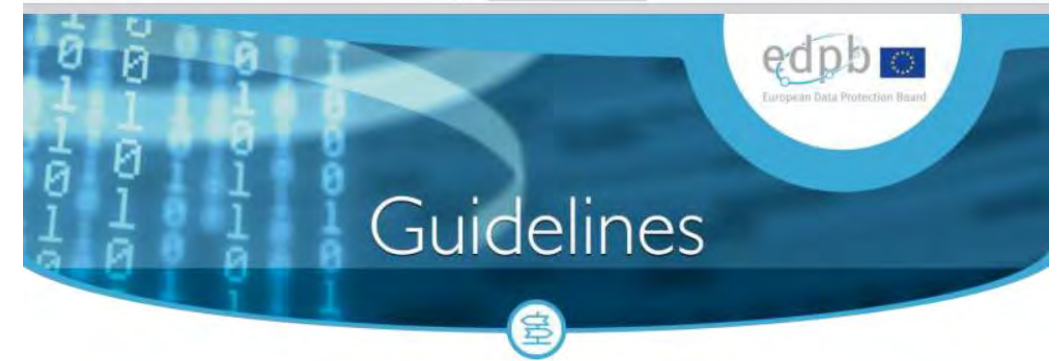
Guidelines 01/2022 on data subject rights - Right of access

Version 2.0

Adopted on 28 March 2023

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 2.0

Adopted on 28 March 2023

Provisional text	
	JUDGMENT OF THE COURT (First Chamber)
	4 May 2023 (*)
	(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Data subject's right of access to his or her data undergoing processing – Article 15(3) – Provision of a copy of the data – Concept of 'copy' – Concept of 'information')
In Case C-487/21,	
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Austria), made by decision of 9 August 2021, received at the Court on 9 August 2021, in the proceedings	
F.F.	
	v
Österreichische Datenschutzbehörde,	
intervening party:	
CRIF GmbH,	
	THE COURT (First Chamber),
composed of A. Arabadjiev, President of the Chamber, P.G. Xuereb, T. von Danwitz, A. Kumin and I. Ziemele (Rapporteur), Judges,	
Advocate General: G. Pitruzzella,	
Registrar: A. Calot Escobar,	
having regard to the written procedure,	
after considering the observations submitted on behalf of:	
– F.F., by M. Schrems,	
– Österreichische Datenschutzbehörde, by A. Jelinek and M. Schmidt, acting as Agents,	

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 ECJ
(Case [C-487/21](#))

- The first sentence of Article 15(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that the right to obtain from the controller a copy of the personal data undergoing processing means that **the data subject must be given a faithful and intelligible reproduction of all those data**. That right entails **the right to obtain copies of extracts from documents or even entire documents or extracts from databases which contain, inter alia, those data, if the provision of such a copy is essential in order to enable the data subject to exercise effectively the rights conferred on him or her by that regulation**, bearing in mind that account must be taken, in that regard, of the **rights and freedoms of others**.

Provisional text	
	JUDGMENT OF THE COURT (First Chamber)
	4 May 2023 (*)
	(Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Data subject's right of access to his or her data undergoing processing – Article 15(3) – Provision of a copy of the data – Concept of 'copy' – Concept of 'information')
In Case C-487/21,	
REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Austria), made by decision of 9 August 2021, received at the Court on 9 August 2021, in the proceedings	
F.F.	
	v
Österreichische Datenschutzbehörde,	
intervening party:	
CRIF GmbH,	
	THE COURT (First Chamber),
composed of A. Arabadjiev, President of the Chamber, P.G. Xuereb, T. von Danwitz, A. Kumin and I. Ziemele (Rapporteur), Judges,	
Advocate General: G. Pitruzzella,	
Registrar: A. Calot Escobar,	
having regard to the written procedure,	
after considering the observations submitted on behalf of:	
– F.F., by M. Schrems,	
– Österreichische Datenschutzbehörde, by A. Jelinek and M. Schmidt, acting as Agents,	

Training of Lawyers on EU Law relating to Data Protection 2



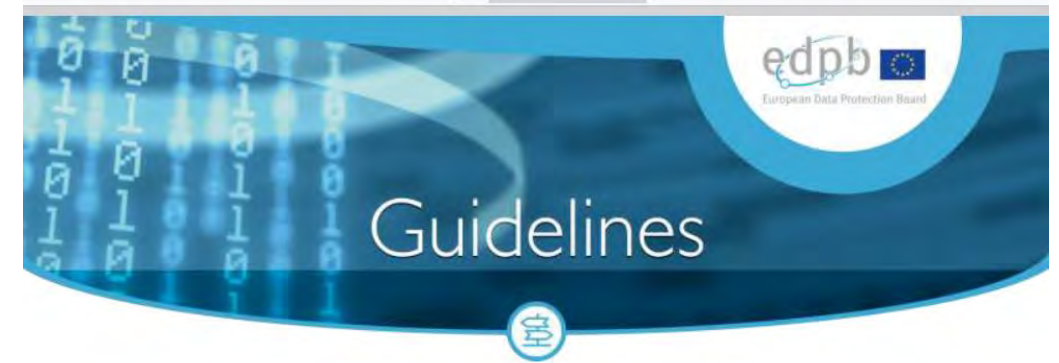
#TRADATA2

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

- The third sentence of Article 15(3) of Regulation 2016/679 must be interpreted as meaning that the concept of ‘information’ to which it refers relates exclusively to the personal data of which the controller must provide a copy pursuant to 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.



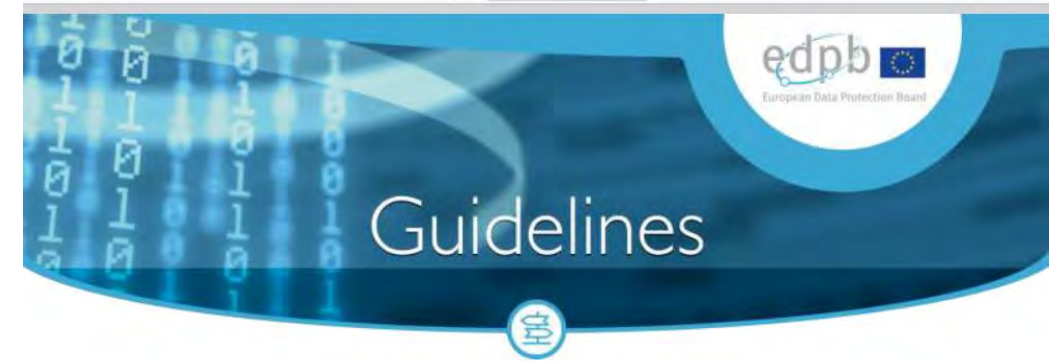
Guidelines 01/2022 on data subject rights - Right of access

Version 2.0

Adopted on 28 March 2023

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 2.0

Adopted on 28 March 2023

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 rights?

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

AI Act

- Algorithmic Transparency obligations

Questions?





Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2

Avv. Giovanni Battista Gallus – gallus@array.law

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

Data protection law enforcement directive

Manuel Martínez Ribas

Palermo, 19 May 2023



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

RULES TO BE CONSIDERED

A. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April (GDPR).

Article 1 Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of **natural persons** with regard to the processing of personal data and rules relating to the **free movement** of personal data.
2. This Regulation protects **fundamental rights and freedoms** of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data **within the Union** shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Art. 2 Material scope

Transfers in certain sectors are based on specific international agreements.

A. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April (GDPR).

The **GDPR** is intended to apply to all processing of personal data in the Member States, both in the public and private sectors, although it does not apply to processing carried out in the exercise of activities that do not fall within the scope of European Union law, such as state **security or national defense activities**, and those **carried out for the purposes of the LED**.

Processing carried out to ensure state security or national defense does not fall within the scope of the European Union and remains governed by the provisions of the **Member States legislation**.

A. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April (GDPR).

Article 2(2)(d) GDPR provides that the Regulation does not apply:

- 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, including the safeguarding against and the prevention of threats to public security’.*

B. THE EU-US TERRORIST FINANCE TRACKING PROGRAMME (TFTP), WHICH TOOK EFFECT ON 1 AUGUST 2010

- An EU-US Agreement on the exchange of financial information ensures protection of EU citizens' privacy and gives the U.S. and EU law enforcement authorities a powerful tool in the fight against terrorism.
- The TFTP has generated significant intelligence that has helped detect terrorist plots and trace their authors.
- A European public authority - [Europol](#) - assesses whether the data requested in any given case are necessary for the fight against terrorism and its financing. Europol also verifies that each request is tailored as narrowly as possible to minimise the amount of data requested. If a request for data does not meet these conditions, no data can be transferred under the Agreement.

C. DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

Article 1 Subject-matter and scope

1. This Directive provides for: (a) the **transfer by air carriers of passenger name record (PNR)** data of passengers of **extra-EU flights**, (b) the processing of the data referred to in point (a), **including its collection, use and retention by Member States** and its **exchange between Member States**.
2. PNR data collected in accordance with this Directive may be processed only for the purposes of **preventing, detecting, investigating and prosecuting terrorist offences and serious crime**.

C. DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

- While airline companies are under a legal obligation to collect and transfer PNR data pursuant to the Directive, they neither exercise public authority nor are entrusted with public powers in that context.
- Accordingly, the **CJEU** has held that they cannot be deemed competent authorities for the purposes of Article 3(7) LED

D. COUNCIL DECISION (EU) 2022/722 OF 5 APRIL 2022 AUTHORISING MEMBER STATES TO SIGN, in the interest of the European Union, the second additional protocol to the convention on cybercrime on enhanced co-operation and disclosure of electronic evidence

- The **Protocol** was signed in the presence of several ministers by the following Council of Europe member states: **Austria, Belgium, Bulgaria, Estonia, Finland, Iceland, Italy, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Portugal, Romania, Serbia, Spain and Sweden**, and by non-member states: **Chile, Colombia, Japan, Morocco and United States**.

E. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters

- Personal data covered by this proposal is protected and may only be processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (Law Enforcement Data Protection Directive)

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

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

- falls **outside of the scope of the GDPR**
- requires transposition, **by 6 May 2018**
- only applies in cases where the **data controller** is a ‘**Competent Authority**’, and the **processing is done for ‘law enforcement purposes’**:
 - a) a public or private body who fits the definition of ‘competent authority’ (such as **local authorities when prosecuting litter fines, or Townhall Bus in relation to ticket offences**). This means that a potentially very large number and variety of bodies might fall under the scope, and the applicability of this regime will need to be assessed on.

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

- b) law enforcement authority may conduct data processing which has nothing to do with its law enforcement function (HR matters, procurement, etc.), and in the latter case, private sector entities may have been entrusted with public authority or be performing data processing contracted out to them by a public authority, where their processing is for law enforcement purposes. a case-by-case basis. (for example, the internal security services of the public transport networks, sports federations approved for the purpose of providing security at sporting events, etc.).

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

- c) **Agencies or units dealing with national security** do not qualify as ‘competent authorities’ within the meaning of Article 3(7) LED, as Recital 14 indicates. Thus, their data processing activities fall outside the scope of application of the Directive. **However, nothing prevents Member States** from broadening the scope of application of their national transposition of the LED so as to cover the activities of national security agencies too. This issue has been raised within the Commission Expert Group on the LED:

Austria / Finland

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

Subject-matter art 1

- the prevention of criminal offences
- the investigation of criminal offences
- the detection of criminal offences
- the prosecution of criminal offences
- the execution of criminal penalties
- Including the protection against threats to public security and its prevention:
- preventive police activities for the purpose of protecting against threats to public security that could lead to a criminal charge (police activities at demonstrations, sporting events, maintaining public order, etc.) and processing operations carried out for these purposes.

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 TRANSPOSITION

- The EU Commission initiated **infringement procedures against 19 Member States in July 2018 (all except one closed in 2020)** for failing to adopt laws transposing the LED by the May 2018 deadline and to duly notify the Commission of their transposition. Another procedure for partial **non-transposition** was initiated in July 2019 against another Member State.
- The Commission reported that while **transposition has been "satisfactory"** there are "a number of outstanding issues" that remain, which resulted in infringement proceedings against **Spain in 2021** (penalty 15 million€ and daily €89,000 - CJEU, because of the seriousness and duration of the infringement) and **Germany** (partial non-transposition, in relation to the activities of Germany's federal police.) **in April 2022**.
- The Commission will continue to assess the transposition of the LED within the Member States and will take the necessary measures to remedy any gaps.

- All but two Member States (**Belgium** and **Sweden**) have entrusted the enforcement of the LED to the supervisory authority that is also responsible for enforcing the GDPR:
 - **Belgium** has entrusted the supervision of the police for the purposes of the LED to a different supervisory authority.
 - In **Sweden** the supervision of certain competent authorities, including the police, is co-shared by the supervisory authority competent for the GDPR and another supervisory authority.
- Furthermore, pursuant to the LED, all data protection supervisory authorities are not competent to supervise the courts when they act in their judicial capacity.

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 - TRANSPOSITION

- Member States have followed different approaches when transposing Article 3 LED at national level.
- The vast majority of Member States (e.g. **Austria, Denmark, Finland, Germany, Italy, Lithuania, Luxembourg and Sweden**) **have reproduced almost verbatim most of the LED definitions in their national law.**
- However, they have typically made some adaptations or introduced new elements when transposing the definition of ‘**competent authority**’.
- Other Member States (e.g. Bulgaria) have transposed Article 3 by simply introducing a cross-reference to the equivalent definitions in Article 4 GDPR in their national legislation.³⁹ Still other Member States (e.g. France) have transposed only a few limited definitions, but left most terms undefined in their national legislation.

First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')

- Practice shows that the number of requests received can vary significantly (e.g. one such request was received in **Croatia**, but more than 1500 were received in **France**).
- While data protection supervisory authorities determined, following a verification or a review of these complaints, that the majority of requests were inadmissible, in several cases, the data controller was ordered either to rectify or erase the personal data, or to restrict the processing of personal data, thereby ensuring the proper application of the restrictions
- Six **Data Protection Supervisory Authorities** reported that they had received no data breach notifications and several others reported that they had received very few such notifications. For example, the **Italian authority reported just three data breach notifications** and the **French authority reported eight**, but the **Dutch authority reported over 500**.

First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')

- Half of the **Data Protection Supervisory Authorities** reported that they had been consulted on data protection impact assessments. The number of prior consultations varies between Member States.
- Some authorities were consulted only once while another authority received 59 prior consultations 129 .
- In most of these cases the **Data Protection Supervisory Authorities** provided written advice and in some cases used their corrective powers in relation to the processing - in particular, they issued warnings or ordered measures to bring the data processing into compliance with the law. In one case, the **Data Protection Supervisory Authority** issued a negative opinion which appears to have had the same effect as a ban on processing.

The European Commission has expressed this in the following terms:

- The processing activities covered by the Directive include the processing activities of police and law enforcement authorities related to threats that may lead to a criminal offence. [...] **On the other hand, processing of HR data of law enforcement authorities, asylum, border control, or processing by the banks is not covered and falls under the GDPR.**

Several **Data Protection Supervisory Authorities** consider that the LED has not been adequately transposed in their countries, and that national law is unclear and incomplete on some issues. One of these issues is the scope of application of the LED, especially as regards data processing operations by judicial, state security, tax, customs and migration authorities, and as regards the processing of data in relation to minor offences and administrative fines, which may fall outside the LED's concept of "criminal offence".

When a court has both a criminal and civil (or administrative) jurisdiction, it is only the personal data processing activities that it carries out for criminal law purposes that are caught by the LED; the rest of the data processing activities are caught by the GDPR.

DIRECTIVE (EU) 2016/680 (“LED”) AND REG. (EU) 2016/679 (“GDPR”)

Some obligations under the Directive are identical to those under the GDPR:

1. implement appropriate **technical and organizational measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Directive (Article 19);
2. implement **data protection by design and by default** (Article 20);
3. use processors that provide **sufficient guarantees and act only on instructions from the controller** (Article 22);
4. maintain a **record of processing activities (R.O.P.A.)** (Article 24);
5. implement **logging measures** (Article 25);
6. **cooperate with the supervisory authority** in the performance of its tasks on request (Article 26);
7. carry out a **data protection impact assessment** when the processing is likely to result in a **high risk** to the rights and freedoms of natural persons (Article 27);
8. consult the supervisory authority in advance in the cases listed in Article 28 of the Directive;

DIRECTIVE (EU) 2016/680 (“LED”) AND REG. (EU) 2016/679 (“GDPR”)

Some obligations under the Directive are identical to those under the GDPR:

9. implement appropriate measures to ensure a level of security appropriate to the risk, in particular as regards **the processing of special categories of personal data** referred to in Article 10 (Article 29);
10. **notify the supervisory authority of a personal data** breach without undue delay, and, where feasible, **not later than 72 hours** after having become aware of it, when the breach is likely to result in a risk to the rights and freedoms of natural persons (Article 30);
11. communicate **the personal data breach to the data subject** without undue delay where the personal data breach is likely to result in a **high risk to his/her rights and freedoms (Article 31);**
12. **designate a data protection officer** under the conditions set out in Article 32 of the Directive;
13. respect the conditions defined for the transfer of personal data to third countries or to international organizations (Article 35 and following).

DIRECTIVE (EU) 2016/680 (“LED”) AND REG. (EU) 2016/679 (“GDPR”)

Some obligations under the Directive are identical to those under the GDPR:

14. where applicable and as far as possible, to make a **clear distinction between personal data of different categories of data subjects**, such as persons convicted of a criminal offence, victims of a criminal offence, other parties to a criminal offence etc. (Article 6);
15. **distinguish between personal data** (personal data based on facts/personal data based on personal assessments) and **ensure the quality of personal data** (Article 7);
16. **processing must be lawful**, i.e. 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 (Article 8);
17. processing of **special categories of data is allowed only where strictly necessary** (Article 10).

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

What rights for data subjects?

Due to the specificity of the scope of the **LED**, some rights included in the **GDPR** are not found in the Directive (**e.g. the right to portability**) or may be subject to limitations. The rights of natural persons recognized in the Directive are as follows:

- information to be made available to the data subject, **subject to possible limitations** (Article 13);
- **the right of access** (Article 14), subject to limitations in whole or in part, in particular in order **not to obstruct investigations, or to avoid prejudicing the prevention or detection of criminal offences, etc.** (Article 15). **In practice, the limitation of the right of access may lead to the implementation of an "indirect right of access", i.e.,**  **exercised through the intermediary of the competent supervisory authority (Article 17);**
- the right to **rectification or erasure** of personal data (Article 16).

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

- Contrary to the GDPR, the LED does not specify whether its rules apply to the **processing of data on deceased persons**. This is particularly remarkable, given that data on deceased persons are ordinarily processed by law enforcement authorities.
- However, by analogy with the GDPR it **would seem reasonable to assume that it is up to Member States to decide whether their national legislation transposing the LED applies to the processing of data on deceased people. In the absence of a clear specification in this sense in the relevant national legislation, it is fair to assume that the LED rules do not apply to the processing of data on deceased individuals**. Presumably, however, the rules would apply to the processing of data on persons about whom there is ongoing uncertainty as to their life status. This would typically be the situation with persons who are reported as missing—at least until a period of time has passed after which it is reasonable for law enforcement agencies to assume that a person is dead (even if their body is not found)

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

- Article 3 LED is to ensure that certain key data protection terms are defined and interpreted uniformly across different EU data protection instruments.
- Barring the definition of ‘competent authority’ in Article 3(7), all of the definitions in Article 3 LED mirror—essentially verbatim—the equivalent definitions in Article 4 GDPR.
- **Consent does not constitute a valid lawful basis under the LED**

The definitions of ‘**referencing**’ and ‘**to make anonymous**’ were omitted too. These terms are no longer used in the LED, though a reference to the notion of ‘anonymous information’ may be found ⁱⁿ recital 21

DIRECTIVE (EU) 2016/680 (“LED”) OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

- For the purposes of the LED, ‘personal data’ does not extend **to biological material as such** (e.g. blood, saliva, hair, or the chemical components of the human body). This follows from **Recital 24**, which distinguishes between bodily samples and the data derived from such samples, and from Article 3(12) and Recital 23, both of which refer to data that ‘result from the analysis of a biological sample’. **The same distinction was made by WP29 with respect to biometric data.**
- Article 3(3) LED takes over the definition in Article 2(c) FD and, in the process of doing so, **it changes the term it defines: from ‘blocking’ to ‘restriction of processing’. **RESTRICTION IS A BROADER CONCEPT.**** ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

EXAMPLE INFORMATION REQUEST



MINISTERIO
DEL INTERIOR



DIRECCIÓN GENERAL
DE LA POLICÍA
CUERPO NACIONAL DE POLICÍA
COMISARÍA GENERAL DE
INFORMACIÓN

OFICIO

S/REF.:

N/REF.: 20220921-184

FECHA: 28 de septiembre de 2022

ASUNTO: Solicitud de información.

DESTINATARIO: [REDACTED]

En el marco de una operación policial que están desarrollando miembros de esta Comisaría General de Información, la cual es necesaria para la prevención, detección e investigación de una infracción penal, en concreto, un delito de terrorismo de los tipificados en el artículo 573 y siguientes del Código Penal, o para la prevención de un peligro real y grave para la seguridad pública, y conforme a lo dispuesto en el artículo 7 de la Ley Orgánica 7/2021, de 26 de mayo, de Protección de Datos Personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, se solicita su colaboración con esta Comisaría General.

El referido artículo 7 de la LO 7/2021, establece en su apartado 2, que *las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública.* Además, en su apartado 4 recoge respecto a este supuesto que *el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.*

Conforme a lo anteriormente expuesto, interesa conocer los datos disponibles en sus entidades de:

- [REDACTED] con número de [REDACTED] nacido el día [REDACTED] en [REDACTED]

La respuesta a la presente solicitud se efectuará al correo electrónico oficial desde el que se remite este escrito: cgi.intel.financiacion@policia.es

Agradeciendo de antemano su colaboración.

EL INSPECTOR, JEFE DE GRUPO



MINISTERIO
DEL INTERIOR



DIRECCIÓN GENERAL
DE LA POLICÍA
CUERPO NACIONAL DE POLICÍA
COMISARÍA GENERAL DE
INFORMACIÓN

OFICIO

S/REF.:

N/REF.: 20220804-171

FECHA: 28 de septiembre de 2022

ASUNTO: Solicitud de información.

DESTINATARIO: [REDACTED]

En el marco de una operación policial que están desarrollando miembros de esta Comisaría General de Información, la cual es necesaria para la prevención, detección e investigación de una infracción penal, en concreto, un delito de terrorismo de los tipificados en el artículo 573 y siguientes del Código Penal, o para la prevención de un peligro real y grave para la seguridad pública, y conforme a lo dispuesto en el artículo 7 de la Ley Orgánica 7/2021, de 26 de mayo, de Protección de Datos Personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, se solicita su colaboración con esta Comisaría General.

El referido artículo 7 de la LO 7/2021, establece en su apartado 2, que *las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública.* Además, en su apartado 4 recoge respecto a este supuesto que *el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.*

Conforme a lo anteriormente expuesto, interesa conocer los datos disponibles en sus entidades de:

- [REDACTED] NIE [REDACTED] nacido el [REDACTED]

La respuesta a la presente solicitud se efectuará al correo electrónico oficial desde el que se remite este escrito: cgi.intel.financiacion@policia.es

Agradeciendo de antemano su colaboración.

EL INSPECTOR, JEFE DE GRUPO



INSPECTOR-
PN:ES-076926
-D.G.POLICIA
(FIRMA)

Firmado
digitalmente por
INSPECTOR-
PN:ES-076926-
D.G.POLICIA (FIRMA)
Fecha: 2022.09.28
10:07:45 +02'00'

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION (ACCORDING TO SPANISH LO 07/2021)

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PURPOSE:

The purpose of the PROTOCOL **is to have a procedure that will provide the minimum measures suggested in order to comply with the obligation provided for in the art 7 LO 07/2021 (SPANISH ORGANIC LAW) , avoiding giving access to personal data to third parties not covered by the regulations in cases not covered by the regulations, or **arising from the failure to comply with the obligation of collaboration in appropriate cases, considered a very serious offense under art. 58, with the potential risk that this brings in terms of sanctions provided for in art. 62 (fine of 360,001 to 1,000,000 euros).****

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

1. **SENDER verification**

a) Must be a Competent Authority according to Spanish LO 07/2021

- i. Security Forces and Corps.
- ii. Penitentiary Administrations.
- iii. The Deputy Directorate of Customs Surveillance of the State Agency of Tax Administration.
- iv. The Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses.
- v. The Commission for the Oversight of Terrorist Financing Activities.
- vi. Judicial authorities of the criminal jurisdictional order and the Public Prosecutor's Office. (including Judicial Police)

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

1. **SENDER verification**

b) It must be verified that the sender is indeed who claims to be

i. **Header verification.**

- The document should be read, identifying the form elements as shown in Annex II.

ii. **Signature of the same.**

- Verification of the validity of the qualified electronic signature.
- Verification that it comes from a qualified Service Provider.
- Verification of the validity of the certificate used.

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

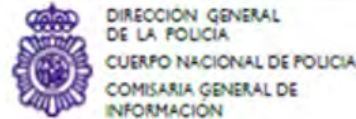
PROCEDURE:

1. **SENDER verification** (DOUBTS??)

In any case, it is convenient to additionally make a telephone communication with the corresponding authority, verifying the origin of the Request in order to exclude cases of identity theft.

ANNEX I

DOCUMENT FORMALITIES



OFICIO

S/REF:

N/REF:

FECHA:

ASUNTO: Solicitud de información.

DESTINATARIO:

Performance Reference, with which it identifies the same

Verify date match.

Verify that it has a specific recipient.

En el marco de una operación policial que están desarrollando miembros de esta Comisaría General de Información, la cual es necesaria para la prevención, detección e investigación de una infracción penal, en concreto, un delito de [REDACTED] de los tipificados en el artículo [REDACTED] siguientes del Código Penal, o para la prevención de un peligro real y grave para la seguridad pública, y conforme a lo dispuesto en el artículo 7 de la Ley Orgánica 7/2021, de 26 de mayo, de Protección de Datos Personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, se solicita su colaboración con esta Comisaría General.

Verify
Motivation:
Relation of
facts and
law.

El referido artículo 7 de la LO 7/2021, establece en su apartado 2, que las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. Además, en su apartado 4 recoge respecto a este supuesto que el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.

Conforme a lo anteriormente expuesto, interesa conocer los datos disponibles en sus entidades de:

- [redacted] NIE [redacted] Pasaporte [redacted] nacido el [redacted] en [redacted]

Verify concrete and specific character. Identification of persons or precise and determined context.

La respuesta a la presente solicitud se efectuará al correo electrónico oficial desde el que se remite este escrito: [redacted]

Verify shipping address to the specific recipient.

Agradeciendo de antemano su colaboración.

Verify signature field. Validity of the signature.

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

2. CONTENT verification

a) The request must be CONCISE AND SPECIFIC

- i. must specify the personal data that directly or indirectly indicate a natural person, about which information is required. From this, it is excluded general considerations to indeterminate groups, which are not massive data requests.

Based on this, a Request that does not clearly indicate personal data allowing the identification of a specific or determinable natural person, alluding to excessively generic references, is not considered to be concrete and specific.

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

2. **CONTENT verification**

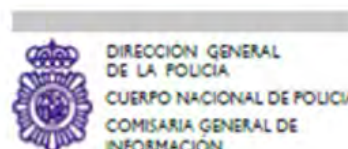
b) The request must be REASONED

- i. Relation and basis of facts and law. Mention of the specific facts and applicable law.
- ii. The Request must state the regulations on which the information is based, as well as a reference to the facts under investigation or their legal qualification.

Therefore, a Request without references to the fact under investigation or **the lack of indication of the specific regulations is not considered to be motivated.**

ANNEX I

DOCUMENT FORMALITIES



OFICIO

S/REF:

N/REF:

FECHA:

ASUNTO: Solicitud de información.

DESTINATARIO:

Performance Reference, with which it identifies the same

Verify date match.

Verify that it has a specific recipient.

En el marco de una operación policial que están desarrollando miembros de esta Comisaría General de Información, la cual es necesaria para la prevención, detección e investigación de una infracción penal, en concreto, un delito de [REDACTED] de los tipificados en el artículo [REDACTED] siguientes del Código Penal, o para la prevención de un peligro real y grave para la seguridad pública, y conforme a lo dispuesto en el artículo 7 de la Ley Orgánica 7/2021, de 26 de mayo, de Protección de Datos Personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, se solicita su colaboración con esta Comisaría General.

Verify
Motivation:
Relation of
facts and
law.

El referido artículo 7 de la LO 7/2021, establece en su apartado 2, que las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. Además, en su apartado 4 recoge respecto a este supuesto que el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.

Conforme a lo anteriormente expuesto, interesa conocer los datos disponibles en sus entidades de:

- [redacted] NIE [redacted] Pasaporte [redacted] nacido el [redacted] en [redacted]

Verify concrete and specific character. Identification of persons or precise and determined context.

La respuesta a la presente solicitud se efectuará al correo electrónico oficial desde el que se remite este escrito: [redacted]

Verify shipping address to the specific recipient.

Agradeciendo de antemano su colaboración.

Verify signature field. Validity of the signature.

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

3. Analyze Exception art. 7

“The provisions of the preceding paragraphs shall not apply when judicial authorization is legally required to collect the data necessary for the fulfillment of the purposes of Article 1” (prevention, detection, investigation and prosecution of criminal offenses or enforcement of criminal penalties, including the protection and prevention of threats to public safety).”

Entry and search of a domicile. /Tapping a telephone line/Install a tracking device. /Others to be determined on a case-by-case basis.

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

4. If the request is approved according to previous steps >> Response to the Request

a) Forward the data, reports, background information and supporting documents to the competent authorities:

- i. With an encryption process to avoid possible leaks. It will be necessary to send the password for decryption through an alternative channel to the one used to send the documents. For example, different email addresses, SMS.
- ii. In an extension as requested by the competent authority.
- iii. Addressed only to the sending Competent Authority.
- iv. Document the process in order to eventually be able to use such proof.

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

4. If the request is NOT approved according to previous steps.

- a) In case of finding that the sender is a competent authority, give an answer arguing the refusal (lack of motivation, lack of precision, case of application of the "judicial authorization" exception). In addition and without confirming or denying, it will be offered that, in the event that data is available, the requested data will be **prudentially “blocked” (RESTRICTED)** in order to guarantee its immutability and restrictive access while awaiting a court order that requires it.

EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

4. If the request is NOT approved according to previous steps.

- b) In case of finding that it is not a competent authority, give an answer alluding to this fact as justification for the refusal.

PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

4. In case of uncertainty as to the merits of the request:

Give an answer alluding to the reasons that generate the situation of uncertainty. Additionally and without confirming or denying, it will be offered that, in the event that data is available, the requested data will be **prudentially “blocked” (RESTRICTED) in order to guarantee its** immutability and restrictive access while awaiting a court order that requires it.

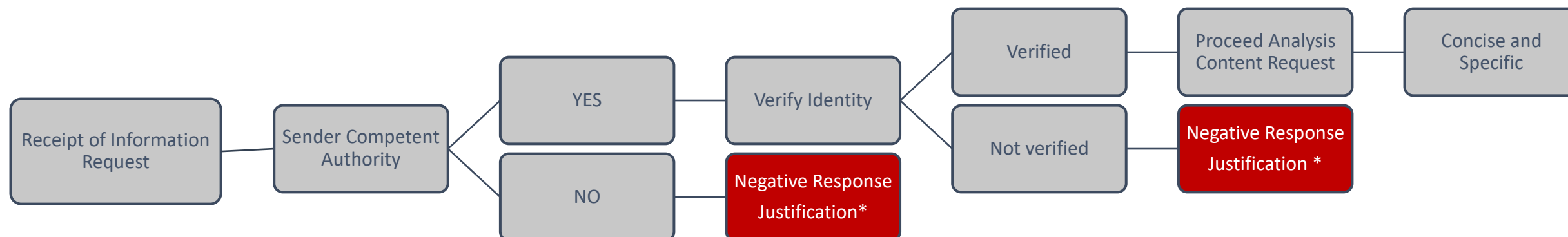
EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

PROCEDURE:

FROM PARAGRAPH 4 OF ART. 7 LO 07/2021, THE DATA SUBJECT SHALL NOT BE INFORMED OF THE TRANSMISSION OF HIS DATA TO COMPETENT AUTHORITIES, NOR OF HAVING PROVIDED ACCESS TO THEM BY SUCH AUTHORITIES IN ANY OTHER WAY, IN ORDER TO ENSURE THE INVESTIGATIVE ACTIVITY.

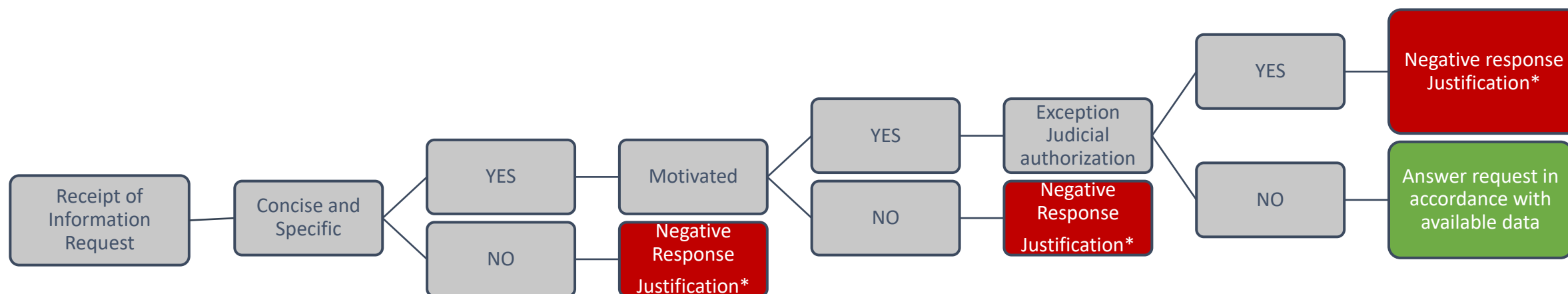
EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

FLOW CHART: PHASE 1



EXAMPLE OF SPANISH PROTOCOL FOR RESPONDING TO A REQUEST FOR INFORMATION

FLOW CHART: PHASE 2



(*) In all those cases of a Justified Negative response, a follow-up on the response of the Sender of the Request must be made.

THANK YOU FOR YOUR ATTENTION !!!



MANUEL MARTÍNEZ RIBAS

Partner – Lawyer IT-IP Department

mmartinez@acrosslegal.com

www.acrosslegal.com

ACROSS LEGAL

Barcelona – Madrid – Valencia – Palma

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

Transfers of personal data to third countries

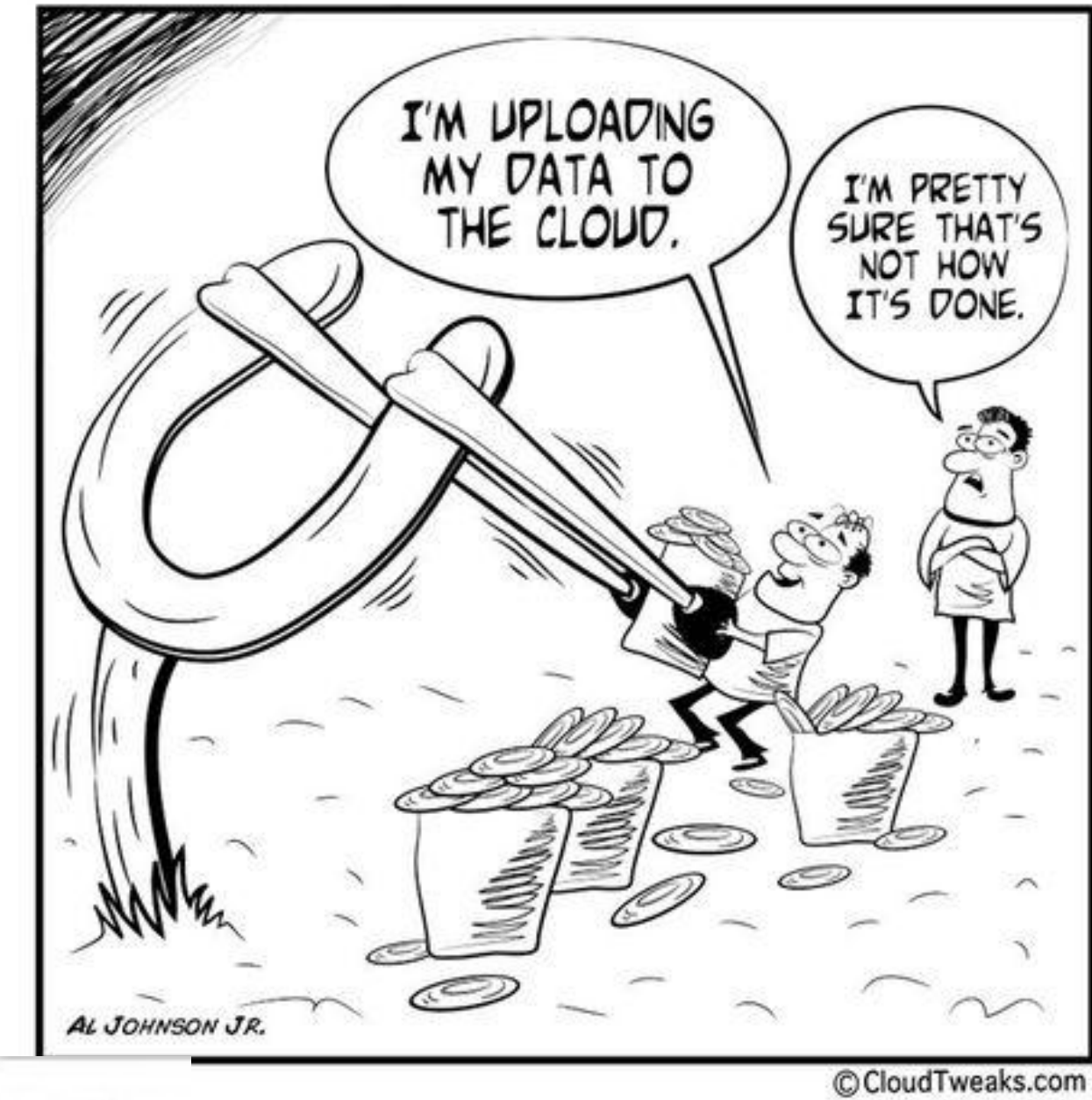
Nicola Fabiano

Palermo, 19 May 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 - 1st 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 - 2nd 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 - 3rd 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.

Guidelines



Guidelines 07/2022 on certification as a tool for transfers

Version 2.0

Adopted on 14 February 2023

These guidelines provide guidance as to the application of Article 46 (2) (f) of the GDPR on transfers of personal data to third countries or to international organisations on the basis of certification. The document is structured in four sections with an Annex.

Article 44 GDPR (General principle for transfers)

Compliance with general provisions of GDPR (in particular Chapter II)

Two-step model.

Compliance with the principles in Article 5 GDPR and if to be verified by a controller in particular lawfulness according to Article 6 GDPR and compliance with Article 9 GDPR (in case of special categories of data).

GDPR transfer toolbox (Chapter V)

Certification as a tool for transfer (appropriate safeguard).
Binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

1.2 General rules applicable to international transfers

4. ... Pursuant to Article 46 (2) (f) of the GDPR, such appropriate safeguards **may be provided for by an approved certification mechanism** 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.
5. As a result, **the data exporter might decide to rely on the certification obtained by a data importer as an element to demonstrate compliance with its obligations e.g. according to Article 24 (3) or Article 28 (5) GDPR. The data importer might decide to apply for certification to demonstrate that appropriate safeguards are in place.**

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:	only if
Subjective scope:	controller and processor
Objective scope:	compliance with conditions
Purposes:	Ensuring the level of protection

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

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

**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 Maximillian 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)



Press release - 28/2/2023

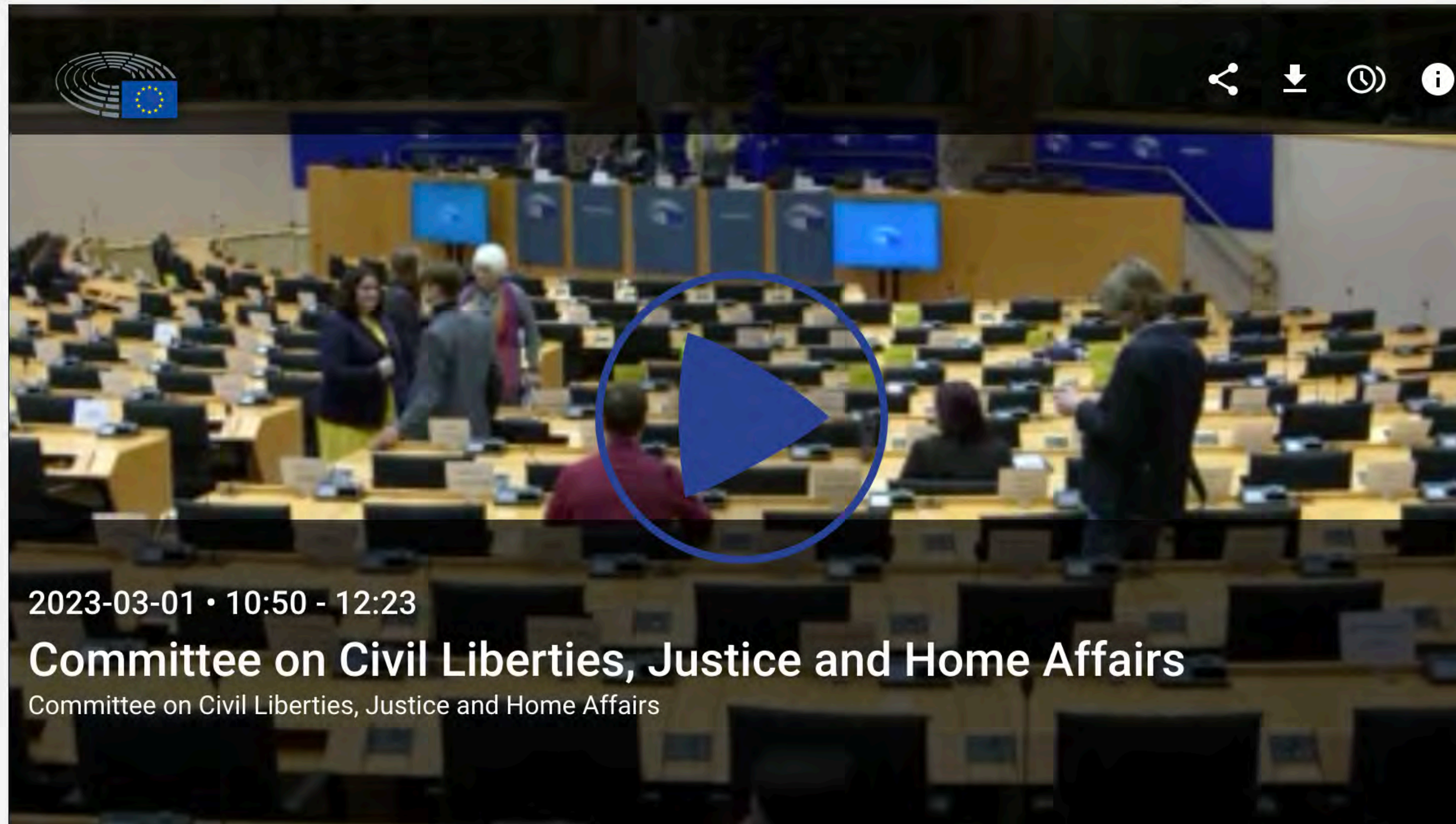
**Opinion 5/2023 on the European Commission Draft
Implementing Decision on the adequate protection of
personal data under the EU-US Data Privacy Framework**

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

Adopted on 28 February 2023



[Home](#) > [Streaming](#) > Committee on Civil Liberties, Justice and Home Affairs



Transfers subject to appropriate safeguards

Transfers subject to appropriate safeguards

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*

Conditions Article 46(1)	Prerequisites: the absence of an adequacy decision	Transfer permissible: only if adequate safeguards are in place and those affected have enforceable data subject rights and effective legal remedies.				
Solution 1: Adequate safeguards Article 46(2)	(a) A legally binding and enforceable instrument between public authorities or bodies;	(b) Binding corporate rules in accordance with Article 47;	(c) Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);	(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);	(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	(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.
Solution 2: Additional appropriate safeguards Article 46(3)*	(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	(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.				
Consistency mechanism Article 46(4)	The supervisory authority shall apply the consistency mechanism referred to in Article 63					

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

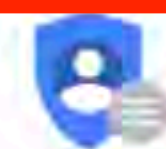
Updates



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](#)

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

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

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

Facebook (Meta) & Privacy Shield

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

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

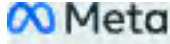
Meta Platforms, Inc. ("Meta") has certified to the [EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework](#) (collectively, "Privacy Shield Frameworks") with the US Department of Commerce regarding the collection and processing of personal data from our advertisers, customers, 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.privacysield.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



Privacy Centre

-  Privacy Centre home
-  Privacy Policy 

What is the Privacy Policy and what does it cover?

What information do we collect?

How do we use your information?

Privacy Policy

What is the Privacy Policy and what does it cover?

Effective from 26 July 2022 | [View printable version](#)

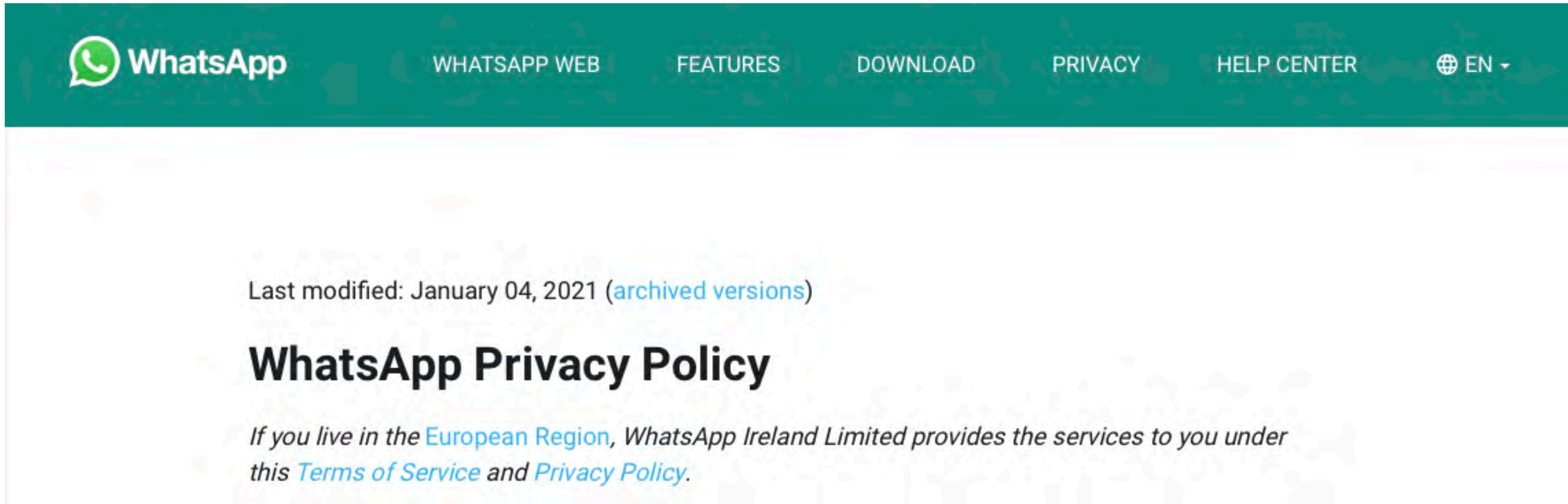
We at Meta want you to understand what information we collect, and how we use and share it. That's why we encourage you to read our Privacy Policy. This helps you use Meta Products in the way that's right for you.

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.

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.

Read the full policy below.

Whatsapp



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

Amazon.com Privacy Notice

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

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

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: privacysshield@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/>

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](#).

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.

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 >](#)



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

Procedure Article 47(1)	Authority: The competent supervisory authority (Lead Authority)	Criterion: Consistency mechanism set out in Article 63	
Conditions Article 47(1)	(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	(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and	(c) fulfil the requirements laid down in paragraph 2.
Content of the BCRs Article 47(2)	The binding corporate rules referred to in paragraph 1 shall specify at least: ... From letter (a) to letter (n)		
Commission's Role Article 47(3)	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).		

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):

Does the Group have its headquarters in the EEA?

☐ Yes
☐ No

Name and location of the applicant:

Identification number (if any):

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

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)

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):

Address:

Country:

Phone number:

Fax:

E-Mail:

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

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](#)

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

The principle of consent
Vincenzo Colarocco
Palermo, 19 May 2023



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

Table of contents

Definition of consent

Elements of Valid Consent

Nature of Consent: Italian and European Jurisprudential Focus

Decisions on The Nature of Consent

Children's Consent and parental liability: Jurisprudential Focus

Marketing and Consent: Italian Jurisprudential Focus

Conclusions

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Elements of valid consent

Pursuant to Article 4 (11) of the EU Regulation 2016/679 ("GDPR") consent is:



Freely given



Specific



Informed



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.

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Elements of valid consent

Freely given

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

- **Conditionality**

The element “free” implies **real choice** and control for data subjects. 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.

- **Granularity**

A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purposes they accept, rather than having to consent to a bundle of processing purposes.

- **Detriment**

The data controller needs to **demonstrate** that it is possible to refuse or to withdraw consent without detriment.

- **Power imbalance**

It is unlikely that public authorities can rely on consent for processing as whenever the controller is a public authority, there is often a clear power imbalance between the controller and the data subject.

Elements of valid consent

Specific

The consent of the data subject must be given in relation to “one or more specific” purposes and that a data subject has a choice in relation to each of them

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2



European Data Protection Board (“EDPB”) Guidelines 05/2020 about consent: to comply with the “specific” element, the controller has to 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 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.

Minimum content requirements for consent to be informed (Guidelines 05/2020):

1. the controller's identity
2. the purpose of each of the processing operations for which consent is sought
3. what (type of) data will be collected and used
4. the existence of the right to withdraw consent
5. information about the use of the data for automated decision-making according to Article 22 (2) where relevant
6. the possible risks of data transfers due to absence of an adequate decision and of appropriate safeguards

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Elements of 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. It must be obvious that the data subject has consented to the particular processing.

A “**clear affirmative act**” means that the data subject must have taken a deliberate action to consent to the processing. Consent can be collected by a written or (a recorded) oral statement, including by electronic means.

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2



Nature of the consent:

Italian and European jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

OVERVIEW OF DECISIONS ON THE NATURE OF CONSENT

Characteristics of consent

Italian Data Protection
Authority –
Provision 4 July 2013

Consent as a unilateral legal act

Cassation Court –
section I, Civil,
Judgement 29 January
2016, n. 1748

Consent is not free if algorithm is unknown

Cassation Court –
section I, Civil, decision
25 May 2021, n. 14381

Consent as informed and conscious choice

European Data Protection
Board ("EDPB") –
Guidelines 03/2022 on dark
patterns in social media
platform interfaces

Nature of the consent:

Italian and European jurisprudential focus

CHARACTERISTICS OF CONSENT

Italian Data Protection Authority – Provision 4 July 2013 Guidelines on Marketing and against Spam

When the company makes registration on its website conditional for marketing purposes, the user's consent is not freely given.

Consequently, the use of its services is illicit, because the data subject cannot make a free choice about the purposes of the data collection.

(<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348>)

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2



Nature of the consent:

Italian and European jurisprudential focus

CONSENT AS A UNILATERAL LEGAL ACT

Cassation Court – section I, Civil, Judgement 29 January 2016, n. 1748

The matter

A company had used the image of a model for advertising purposes without her consent. Specifically, the model had first entered into a contract with the company for photo's publication. When she realised that her photos were being passed on to third parties, she revoked her consent.

Case law

"The consent, as an expression of **the right of personality**, even if occasionally included in a contract, stays distinct and autonomous from the agreement that contains it and is always **revocable**, whatever the term possibly indicated for the permitted publication and regardless of the agreed agreement, which does not integrate an element of the authorization transaction".

(https://www.previti.it/storage/app/media/Documenti%20ufficiali/Sentenza_Cass_civile1748.pdf)

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2



Nature of the consent:

Italian and European jurisprudential focus

CONSENT IS NOT FREE IF ALGORITHM IS UNKNOWN

Cassation Court – section I, Civil, Decision 25 May 2021, n. 14381

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

The matter

A company had developed a method for **rating** and reviewing **people**, especially professionals. The web platform and its computer archive was aimed at developing the **reputational profiles** of natural persons and legal entities. This was to ensure that artificial and fake profiles were not created, by using an algorithm of impartial calculation of the '*reputational rating*' of the analysed subjects, to allow verification of their real credibility when concluding contracts or managing economic relations.

Case law

In the case of web platforms structured on a computational system with an algorithm at its base aimed at establishing reliability scores, the requirement of awareness cannot be considered fulfilled where the executive scheme of the algorithm and the elements of which it is composed remain unknown or unknowable by the interested parties.

(<https://juriswiki.it/wp-content/uploads/2021/05/cassazione-civile-i-sentenza-14381-2021.pdf>)



Nature of the consent:

Italian and European jurisprudential focus

CONSENT AS INFORMED AND CONSCIOUS CHOICE

European Data Protection Board – Guidelines 03/2022 on dark patterns in social media platform interfaces

Dark patterns are techniques implemented on online platforms aimed at inducing users to make unintended, unintentional or potentially harmful decisions regarding the processing of personal data: in particular, they are able to **influence user's behaviour** to hinder the ability to manage personal data and make informed choices.

The EDPB recalls that it is necessary to provide the user with a series of minimal (but not excessive) information, as well as to allow, then, an easy revocation of the same on par with the preliminary release, to reach the threshold of a so-called **informed and free consent** (as a clear, affirmative and unambiguous act)

(https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en)

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2



Nature of the consent:

Italian and European jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

OVERVIEW OF DECISIONS ON ACQUIRING AND WITHDRAWING CONSENT

Methods to withdraw consent

Italian Data
Protection Authority
– Provision 4 July
2013

Active behaviour of the data subject

Court of Justice of
the European Union,
Section II, 11
November 2020 n.
61/19

Consent acquired by clear affirmative act

Italian Data Protection
Authority – Cookies
Guidelines 10 June 2021

Scrolling and cookie walls

European Data
Protection Board,
Guidelines 5/2020

Insufficient transparency in communication templates

Italian Data Protection
Authority –
Provision 23 February
2023

Nature of the consent:

Italian and European jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Methods to withdraw consent

Italian Data Protection Authority –
Provision 4 July 2013

The ways in which consent can be **revoked** can be various and even different from those used to express consent, provided that they express the will of the interested party **without formalities**.
(<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348>)



Active behaviour of the data subject

Court of Justice of the European Union, Sez. II, 11
November 2020 n. 61/19

Data controller must be able to demonstrate that data subject gave the consent to the processing of his personal data, after having first obtained and read the privacy policy by means of active conduct. The Court censured the method of getting consent by means of a **pre-selected tick box**, because that activity does not mean a user's active conduct on the website (<https://curia.europa.eu/juris/liste.jsf?language=it&td=ALL&num=C-61/19>)

Nature of the consent:

Italian and European jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Consent acquired by clear affirmative act

Italian Data Protection Authority – Cookies Guidelines 10 June 2021

Consent can be rightly expressed if it is the result of an affirmative, **conscious action** by the data subject and if **that action** can be appropriately identified and **demonstrated** so that the consent in question can be ultimately considered to be in line with all the requirements set out in the EU Regulation 2016/679. GDPR states that consent is to be free, informed, unambiguous and specific to each different purpose of the processing.
(<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876>)



Nature of the consent:

Italian and European jurisprudential focus



Scrolling and cookie walls

European Data Protection Board, Guidelines 05/2020

Actions such as scrolling or swiping through a webpage or similar user activity will **not** under any circumstances **satisfy the requirement of a clear and affirmative action**: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it. (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it)

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls).

Nature of the consent:

Italian and European jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Insufficient transparency in communication templates

Italian Data Protection Authority – Provision 23 February 2023

The adoption of **unclear communication templates** regarding interfaces' design and ways to get consent is non-compliant with the European Data Protection Regulations. In fact, the use of **dark patterns** designed to tamper data subjects' will gets to greater opacity in the manner in which consent is given. Then data subjects will give consent not by conscious choice. When consent is obtained in such a way as to violate the rule, in fact, data subject is never free to express his or her consent, therefore this and can never be considered lawful.

(<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870014>)



Children's Consent and parental liability

Jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

The lawfulness of the child's consent

European Data Protection Board, Guidelines 05/2020

- In cases relating to provision of information society services for children, consent to the processing of a child's personal data is lawful if the child is at least **16 years old**.
- If the child is **under 16 years old**, the processing will be lawful only if consent is given or authorized **by the holder of parental responsibility** over the child.

Derogation → member States can provide by law a lower age, but this age cannot be **below 13 years**.
Italy → 14 years

Children's Consent and parental liability

Jurisprudential focus

Consent collected without adequate checks on the age of the giver is not valid.

Italian Data Protection Authority – Provision n. 20/2021

The Italian Data Protection Authority has ordered **TikTok to block** the processing of personal data of users whose age the social network cannot prove.

Specifically, TikTok stated that it processed the personal data of all its users on the basis of a contract for the sole purpose of executing the contract. In addition, the social network claimed to process users' data for further commercial purposes through their consent.

The same company identifies its service as restricted to those over the age of thirteen and on this basis proposes that only users who are 13 years old to accept its proposal.

The decision: in the absence of adequate checks on the age of those who accept its contractual proposal and those who give consent to further processing for commercial purposes there is a violation of GDPR rules.

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524194>

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Children's consent and parental liability

Jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2

 #TRADATA2

Parental consent for children under the age of 15

*French Data Protection Authority –
Recommendation n. 7 for enhancing
online children's protection 9 June 2021*

To process data for online services, the holder(s) of parental authority must give consent jointly with the consent of the child if the child is under the age of 15. This means that consent for additional features such as on a social network or on an app must derive from the **mutual consent of the child and the parental authority holder(s)**.
(<https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee>)



Child protection and privacy

*French Data Protection Authority ("CNIL")-
Opinion on age verification systems 26 July
2022*

CNIL supports the logic of parental control, which implies a responsibility on the part of the family to limit access to sensitive content. Despite the complexity, the **intervention of third party providers of a dual authentication system** can be a solution to verify age with a high degree of certainty and protect children's privacy
(<https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie>)

Children's consent and parental liability

Jurisprudential focus

Code of conduct on online child protection

English Data Protection Authority – Age appropriate design code 2 September 2021

The code sets 15 cumulative age-appropriate design standards that reflect a **risk-based approach**. The aim is to provide default settings that guarantee children the best possible access to online services, **to minimize data collection**. The code ensures that children who choose to change default settings receive the right information, guidance and advice in advance, and that they subsequently receive adequate protection regarding the use of their data.

(<https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>)



Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Children's data and parental consent

Irish Data Protection Authority – My child's data protection rights 2022-2027 regulatory strategy

Parental consent is always required when an online business seeks to process the data of a child under the age of 16 on the basis of consent. When a **different legal basis** is used, parental consent may not be necessary, for example, when the purpose is to share the child's data with third parties. Nonetheless, a solid legal basis – **other than consent** – and compliance with the principles of transparency and adequate information will be required.

(<https://dataprotection.ie/en/dpc-guidance/my-childs-data-protection-rights>)

Children's Consent and parental liability

Jurisprudential focus

Obligations of online service providers when the subject is a minor.

European Parliament – Digital Services Act 19 October 2022

DSA emphasises that the protection of minors is an important policy objective of the Union. An online platform can be considered accessible to minors when its general conditions allow minors to use the service. Providers of online platforms accessed by minors must take appropriate and proportionate measures to protect them, for example by **designing their online interfaces** or parts thereof with the highest level of privacy, security and default **safety measures**, as appropriate, or by adopting **standards for the protection of minors**, or by adhering to codes of conduct. For example, providers of intermediary services primarily intended for minors should make special efforts to make the explanation of their general conditions easily understandable to minors. Online platform providers should **not present profiling-based advertising** on their interface that uses the personal data of the service recipient if they know, with reasonable certainty, that the service recipient is a child. (<https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065>)

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Children's Consent and parental responsibility

Jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Parents' role in children's online safety.

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9531639>

The Italian Data Protection Authority has long been campaigning to raise awareness about the protection of children online.

In addition to keeping a high profile on how social networks protect children, the Italian Authority has focused on the role of parents.

The protection of children online must take place in a synergistic manner:

- a) **socials must set up systems** that really manage to ensure that those who open a profile are of the age to do so, at least 14 years old in Italy;
- b) the fundamental **role of parents** in supervising and controlling children from the many dangers of the Web.

Marketing and consent

Italian and European jurisprudential focus

OVERVIEW OF DECISIONS ON ACQUIRING AND WITHDRAWING CONSENT

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Supreme Court of Cassation

- **Consent recovery** – Cassation Court – section I, Civil, decision n. 11019/2021

Italian Data Protection Authority

- **Consent is required in electronic communications for promotional purposes** – Provision n. 52/2018
- **Necessity of consent for database transfer** – Provision n. 19/2018
- **Necessity of consent for telemarketing and teleselling activities** – Provision n. 232/2019
- **Granularity and clarity requirements for requesting consent** – Provision n. 332/2021
- **denied consent should be noted immediately**– Provision n. 431/2022
- **Double opt-in when the will of the person concerned is difficult to prove**– Provision n. 51/2023

Italian jurisprudential focus

Italian Data Protection Authority

PROVISION N. 52/2018

Consent is required in electronic communications for promotional purposes

Electronic communications sent to professionals are characterized by promotional purposes, and it is not possible to send such communications without prior consent, even if personal data are taken from public registers, lists, websites acts or documents known or knowable by anyone.

PROVISION N. 19/2018

Necessity of consent for database transfer

In the case of database transfer, the transferee must send to the data subject a privacy disclaimer, in which he specifies the origin of the data. In this way, each data subject will also be able to address the entity that collected and communicated the data to object to the processing.

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

PROVISION N. 232/2019

Necessity of consent for telemarketing and teleselling activities

The Authority declared the unlawfulness of transfers of personal data carried out by data controllers who have not obtained specific consent directly from the data subjects for telemarketing and teleselling activities.

PROVISION N. 332/2021

Granularity and clarity requirements for requesting consent

A one-time consent to data disclosure for promotional purposes also by group companies, holding, subsidiary and associated companies and possible business partners cannot be considered either specific or free and therefore does not constitute a suitable legal basis for processing.

Italian jurisprudential focus

Italian Data Protection Authority

PROVISION N. 431/2022

Denied consent should be noted immediately

If the user says "**no**" to the unwanted business call, the call center or company that contacted him or her must **immediately** note his or her wishes and delete the name from the lists used for telemarketing." The Authority specified that the right can be exercised "at any time," including during the promotional phone call, and the user's will must be properly recorded. **'Opposition expressed during the phone call does not have to be confirmed by email or other means,** as operators are often asked to do, and is also valid for future promotional campaigns.

(<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9856345>)

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

PROVISION N. 51/2023

Double opt-in when consent is difficult to prove

Double opt-in mode to collect consent is not a legal obligation but, as the Authority said many times, it must be considered an **appropriate measure to prove data subject's consent.** it is a best practice strongly recommended especially when the acquisition of consent to send promotional messages is hard to prove.

(<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870014>)

Italian jurisprudential focus

Cassation Court – section I, Civil

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Provision N. 11019/2021

Consent recovery

The Court ruled that the '**consent recovery**' campaign aimed at obtaining the green light to use the data of customers who **had previously refused** to be contacted by telephone for promotional purposes **violates privacy**: "a telephone communication aimed at obtaining consent for marketing purposes, from someone who has previously refused it, is itself a "commercial communication".

In fact, the consent required for processing is necessarily linked to processing's purposes.

In this case, the company didn't respect users' will, because it reached them without a proper legal basis. (https://images.go.wolterskluwer.com/Web/WoltersKluwer/%7B79d73978-263b-4d05-ad4a-d14613eb3b1b%7D_cassazione-civile-ordinanza-11019-2021.pdf)

Conclusions

1. Consent represents the principal element to express people's will
2. Consent must be **freely given, specific, informed** and **unambiguous**
3. Both Italian and European jurisprudence have explored the nature of consent: a **free unilateral act** that can always be **revoked**, given through a **clear affirmative action**
4. Consent is also essential for **marketing** activities: Italian case law pointed out that consent is required in **electronic communications** for promotional purposes, in **telemarketing** and **teleselling** activities, or even in **database transfer** activities
5. Consent is not only the legal basis for the processing of personal data. It represents **one of the most important way** to protect data subject **freedoms** and **rights**, as the broadest expression of the principle of individual self-determination.

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

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

STUDIO  PREVITI
LEGALE ASSOCIATO ROMA - MILANO

Thank you!

Vincenzo Colarocco, Att.



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