

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

**The Directive 2016/680
Miroslav Krutina**

Rome, 30 September 2022



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

Problems of the Framework decision

- the Directive repeals **Council Framework Decision 2008/977/JHA**, which also regulated the processing of data in the field of police and judicial cooperation in criminal matters
- however, it
 - was **limited in scope**, as it applies only to cross-border data processing and not to the processing of data by police and judicial authorities at purely national level
 - suffered from a lack of harmonisation, leaving Member States considerable freedom in application
 - did not create advisory groups for common interpretation of its provisions

History of the adoption of the Directive

- 2009 - The European Council requests the Commission to evaluate the functioning of the EU data protection instruments
- 2010 - The Commission issues a Communication "A comprehensive approach to data protection in the European Union,,
- 2009-2011 - Consultations with experts and Member States
- 2014-2016 - Legislative process in the European Parliament

Directive (EU) 2016/680

- part of package issued to overhaul the legal framework for data protection in the European Union
 - together with REGULATION (EU) 2016/679 (GDPR)
 - and Directive 2016/681

Objectives of the Directive

- to ensure a high level of harmonized protection of personal data
- thereby increasing mutual trust in the area of personal data protection

Applicability of the Directive

- the activities of the police or other law enforcement authorities in the prevention, investigation, detection and prosecution of crime
- execution of criminal sanctions (and custodial measures)
- enforcement of powers through coercive measures, such as police action during demonstrations, major sporting events and riots
- if personal data is processed for purposes other than those mentioned above, the General Data Protection Regulation applies

Applicability of the Directive

- The Directive does not apply to
 - the exercise of activities not covered by European Union law
 - e.g. activities of national security agencies
 - processing of personal data by the European Union institutions

Affected authorities

- Police
- Courts
- Public Prosecutor
- Ministry of Justice
- Prison service
- Probation and mediation service
- and others...

Public access to official documents

- the Directive is not affecting the principle of public access to official documents
 - the documents may be disclosed in accordance with Regulation (EU) 2016/679 – GDPR
 - or according to the law of the Member States
 - In the Czech Republic, for example, Act No. 106/1999 Coll., on free access to information

Implementation of the Directive in the Czech Republic

- Explanatory memorandum of the Czech Republic: *„The proposed legislation is in line with known good practice. Its procedures, processes and sanctions are in line with existing legislation. The proposed law does not introduce new, innovative practices, but uses existing proven practices.,,*
- The implementation of Directive 2016/680 was subject to meeting demanding financial, technical and personnel requirements relating to the protection of personal data, such as:
 - ensuring database security
 - the cost of data protection assessments in other countries
 - the cost of the Data Protection Officer
 - cost of implementing enhanced data subjects' rights

Content of the Directive

- Chapter I – General provisions
- Chapter II – Principles
- Chapter III – Rights of the data subject
- Chapter IV - Controller and processor
 - Section 1 – General obligations
 - Section 2 – Security of personal data
 - Section 3 - Data protection officer
- Chapter V - Transfers of personal data to third countries or international organisations
- Chapter VI - Independent supervisory authorities
 - Section 1 - Independent status
 - Section 2 - Competence, tasks and powers
- Chapter VII – Cooperation
- Chapter VIII - Remedies, liability and penalties
- Chapter VIII - Implementing acts
- Chapter X – Final provisions

Principles of personal data processing

(Article 4 of the Directive)

- Personal data must be
 - processed in a legal and fair manner
 - collected for specific, articulated and legitimate purposes
 - proportionate, relevant and limited to what is necessary for the purposes for which they are processed
 - accurate and, if necessary, up-to-date
 - kept only for as long as necessary to fulfil their purpose
 - properly secured

Transfer of personal data

- to member states
 - takes place on the basis of **mutual trust**, which is based on the implementation of the Directive
- to third countries or international organisations
 - addressed in Articles 35-40 of the Directive
 - conditions:
 - the purposes are in accordance with the Directive
 - are transferred to authority competent in the scope of the Directive
 - The Commission has decided that this country provides a sufficient level of protection
 - or if guarantees have been provided
 - or exceptions under Article 38

Case Law - Case C-205/21

- Opinion of Advocate General G. Pitruzzell delivered on 30 June 2022:
 - Article 10 of Directive 2016/680 interpreted as meaning that the collection and processing of biometric and genetic data, such as photographs, fingerprints and DNA samples, as a serious interference with the right to the protection of personal data, is permitted only where it is **strictly necessary for the pursuit of objectives related to serious crime**, which must be clearly defined by national law.
 - **The nature and amount of personal data processed must be strictly relevant and consistent with the aims and purposes pursued.** It must also specify the reasons why the processing of such data, in particular genetic data, for that purpose appears necessary despite the fact that it is a serious interference. In addition, national law must clearly set out the conditions for processing in all its aspects, that is to say, from the conditions for collection to the conditions for access to and deletion of the data, by specifying the personal scope of the collection and processing measures in a precise and necessarily strictly limited manner. Each of these conditions must be limited to what is strictly necessary. The regime thus defined must be capable of effectively protecting individuals against the risks of abuse posed in particular by the processing of genetic data.

Case Law - Case C-180/21

- In this case, the Court must answer the Bulgarian court's doubts about the interpretation of the GDPR and Directive 2016/680 in order to clarify, whether there is unlawful processing of personal data held by the public prosecutor's office of a Member State in a situation where
 - firstly, the data was obtained from a person who initially acted as a victim but was later charged in the same criminal proceedings.
 - Secondly, the prosecution seeks to use in its defence data obtained in several criminal proceedings as evidence against a civil action in which the owner of the data seeks compensation for undue delay in criminal proceedings.

Case Law - Case C-180/21

- Opinion of Advocate General M. Campos Sánchez-Bordon delivered on 19 May 2022
 - Article 4(2) of Directive (EU) 2016/680 of the European Parliament and of the Council must be interpreted as meaning **that data obtained from a person who is an alleged victim of a criminal offence, collected in the context of criminal proceedings, are processed for the same purpose as that which justified their collection when that person is subsequently charged in the same criminal proceedings**
 - The communication of personal data collected in the course of criminal proceedings, preceded by their recording, storage and consultation, for the purpose of defending the public prosecutor in civil proceedings in which compensation is claimed for damage resulting from his activities in the performance of his tasks, constitutes 'processing of personal data' within the meaning of Article 4(1) of Regulation 2016/679.

Other Case Law

- Judgment of the Supreme Administrative Court of the Czech Republic of 18 November 2020, No 4 Azs 246/2020-27
- Judgment of the Municipal Court in Prague of 21 July 2022, No 6 A 18/2020-86
- Report of the Office for Personal Data Protection of the Czech Republic on the inspection of the Probation and Mediation Service in the processing of personal data in the execution of the control of the sentence of house arrest in 2018
- + Judgment of the Court of Justice of the EU of 25 February 2021, Case C-658/19

Thank you for your attention

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

Transfers of personal data to third countries
Nicola Fabiano

Rome, 30 September 2022



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

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)*

?

Transfers of personal data to third countries or international organisations

(6) Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

Transfers of personal data to third countries or international organisations

Is that regulation in the GDPR only in Chapter V?

Transfers of personal data to third countries or international organisations

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

...

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular **recipients in third countries or international organisations;**

Transfers of personal data to third countries or international organisations

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

...

d) the categories of recipients to whom the personal data have been or will be disclosed **including recipients in third countries or international organisations;**

Transfers of personal data to third countries or international organisations

Article 40

Codes of conduct

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

...

j) the transfer of personal data to third countries or international organisations; or

...

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 **in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2)**. Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

Transfers of personal data to third countries or international organisations

Article 96

Relationship with previously concluded Agreements

International agreements involving **the transfer of personal data to third countries or international organisations** which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Convention 108/1981

Chapter III – Transborder flows of personal data

Article 14 – Transborder flows of personal data (ex art. 12)

1. A Party **shall not, for the sole purpose** of the protection of personal data, **prohibit or subject to special authorisation the transfer** of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation.
2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, **the transfer of personal data may only take place** where an appropriate level of protection based on the provisions of this Convention is secured.
3. An **appropriate level of protection** can be secured by:
 - a) the law of that State or international organisation, including the applicable international treaties or agreements; or
 - b) ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.
4. Notwithstanding the provisions of the previous paragraphs, **each Party may provide that the transfer of personal data may take place if:**
 - a) the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or
 - b) the specific interests of the data subject require it in the particular case; or
 - c) prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or
 - d) it constitutes a necessary and proportionate measure in a democratic society for freedom of expression.
5. Each Party **shall provide that the competent supervisory authority** within the meaning of Article 15 of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c.
6. Each Party **shall also provide that the supervisory authority is entitled** to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.

Transfers of personal data to third countries or international organisations

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.**

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

General principles

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

General principles

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or in ternational organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

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 - crit. n. 1

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 - crit. n. 2

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 - crit. n. 3

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 - Consequences

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.

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

Has anything changed since Directive 95/46/EC?

Comparative reading

GDPR

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place **where the Commission has decided** that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
 - (a) **the rule of law**, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
 - (b) **the existence and effective functioning of one or more independent supervisory authorities** in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
 - (c) **the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments** as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Directive 95/46/EC

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. **The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations**; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. **Where the Commission finds**, under the procedure provided for in Article 31 (2), **that a third country does not ensure an adequate level of protection** within the meaning of paragraph 2 of this Article, **Member States shall take the measures necessary** to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. **The Commission may find**, in accordance with the procedure referred to in Article 31 (2), **that a third country ensures an adequate level of protection** within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
Member States shall take the measures necessary to comply with the Commission's decision.

Outline on the adequacy decision

The first phase (evaluation) - art. 45(1)(2)

- 1. **Authority:** European Commission
- 1. **Judgement:** unquestionable of the European Commission
- 1. **Subject of judgment:** ensuring an adequate level of protection
- 2. **Assessment elements:**
 - 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 (issuance of the writ of execution) - art. 45(3)

- 3. **Duration of the implementing act:** temporary of 4 years (periodic review)
- 3. **Content of the implementing act:** geographical and sectoral scope and, where possible, identify the supervisory authority or authorities - art. 45(2)(b)
- 3. **Procedure for adopting the implementing act:** committee procedure - art. 93(2)

The third phase (control) - art. 45(4)

- 4. **Powers of the Commission:** monitoring on an ongoing basis
- 4. **Scope of control:** Decisions taken under § 3 and Art. 25, § 6 of Directive 95/46/EC

The fourth stage (control outcome) - art. 45(5)(6)(7)

- 5. **Possible outcome of the review:** revocation, modification or suspension of the adequacy decision without retroactive effect (without prejudice to transfers under § 7)
- 5. **Procedure:** procedure under art. 93(2) or in cases of urgency under art. 93(3)
- 6. **Solutions:** consultations with the third country or international organisation to remedy

The fifth phase (Legal publication) - art. 45(8)

- 8. **Legal publication:** Official Journal of the European Union and EU Commission website.

Previous decisions - art. 45(9)

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

Art. 93 GDPR

Article 93 Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

Regulation (EU) 182/2011

Article 3 - Common provisions

2. The Commission shall be assisted by a committee composed of representatives of the Member States. The committee shall be chaired by a representative of the Commission. The chair shall not take part in the committee vote.

Article 5 - Examination procedure

Article 8 - Immediately applicable implementing acts

1. By way of derogation from Articles 4 and 5, a basic act may provide that, on duly justified imperative grounds of urgency, this Article is to apply.
2. The Commission shall adopt an implementing act which shall apply immediately, without its prior submission to a committee, and shall remain in force for a period not exceeding 6 months unless the basic act provides otherwise.
3. At the latest 14 days after its adoption, the chair shall submit the act referred to in paragraph 2 to the relevant committee in order to obtain its opinion.
4. Where the examination procedure applies, in the event of the committee delivering a negative opinion, the Commission shall immediately repeal the implementing act adopted in accordance with paragraph 2.
5. Where the Commission adopts provisional anti-dumping or countervailing measures, the procedure provided for in this Article shall apply. The Commission shall adopt such measures after consulting or, in cases of extreme urgency, after informing the Member States. In the latter case, consultations shall take place 10 days at the latest after notification to the Member States of the measures adopted by the Commission.

The adequacy decision

(103) The Commission **may decide** with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission **may also decide**, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

The adequacy decision

(107) The Commission **may recognise** that a third country, a territory or a specified sector within a third country, or an international organisation **no longer ensures** an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation **should be prohibited**, unless the requirements in this Regulation relating to transfers subject to **appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled**. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

The adequacy decision

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168) The examination procedure should be used for the adoption of implementing acts on **standard contractual clauses** between controllers and processors and between processors; **codes of conduct**; **technical standards and mechanisms for certification**; the **adequate level of protection** afforded by a third country, a territory or a specified sector within that third country, or an international organisation; **standard protection clauses**; **formats and procedures** for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; **mutual assistance**; and **arrangements for the exchange of information** by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The **Commission should adopt immediately applicable implementing acts** where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation **does not ensure** an adequate level of protection, and imperative grounds of urgency so require.

Transfers subject to appropriate safeguards

Transfers subject to appropriate safeguards

Conditions - art. 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 - art. 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 - art. 46(3) with the authorisation of the supervisory authority

- (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 - art. 46(4)

The supervisory authority shall apply the consistency mechanism referred to in Article 63

Previous authorizations - art. 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

Transfers subject to appropriate safeguards in Directive 95/46/CE

Article 26(4), Directive 95/46/EC

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, **Member States shall take the necessary measures to comply with the Commission's decision.**

Transfers subject to appropriate safeguards

(108) In the absence of an adequacy decision, **the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject.** Such appropriate safeguards may consist of making use of **binding corporate rules, standard data protection clauses** adopted by the Commission, **standard data protection clauses** adopted by a supervisory authority or **contractual clauses** authorised by a supervisory authority. **Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects** appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

Transfers subject to appropriate safeguards

(109) The possibility for the controller or processor to use **standard data-protection clauses adopted by the Commission or by a supervisory authority** should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. **Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.**

Transfers subject to appropriate safeguards

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, **the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights** as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

Adequacy decisions

European Commission website

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

Transfers EU-USA

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.**

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.**

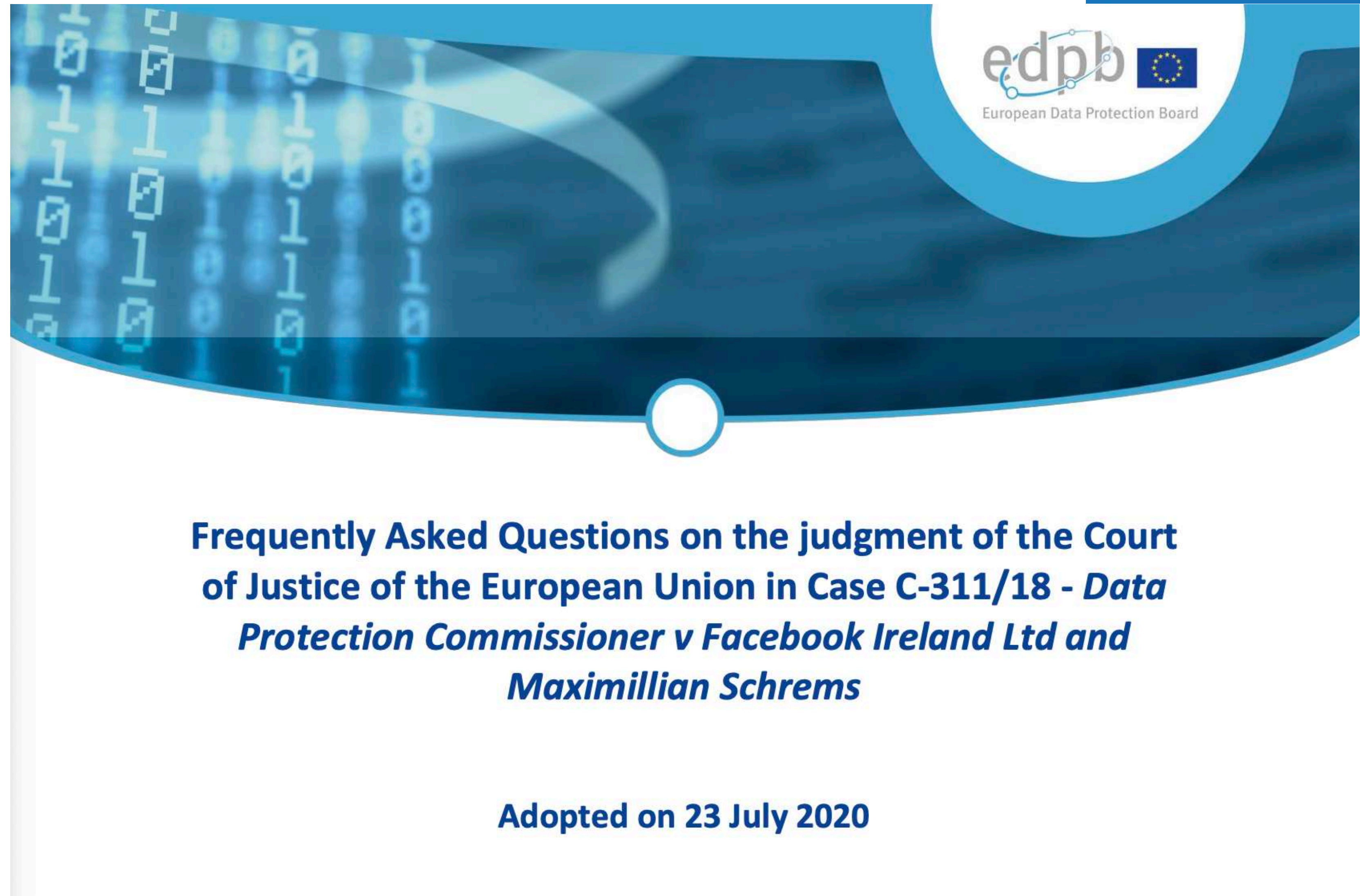
The EDPB position

[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

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 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.

That decision - published in the OJEU of 7/6/2021 - 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 that were 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

- ➔ 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](#)

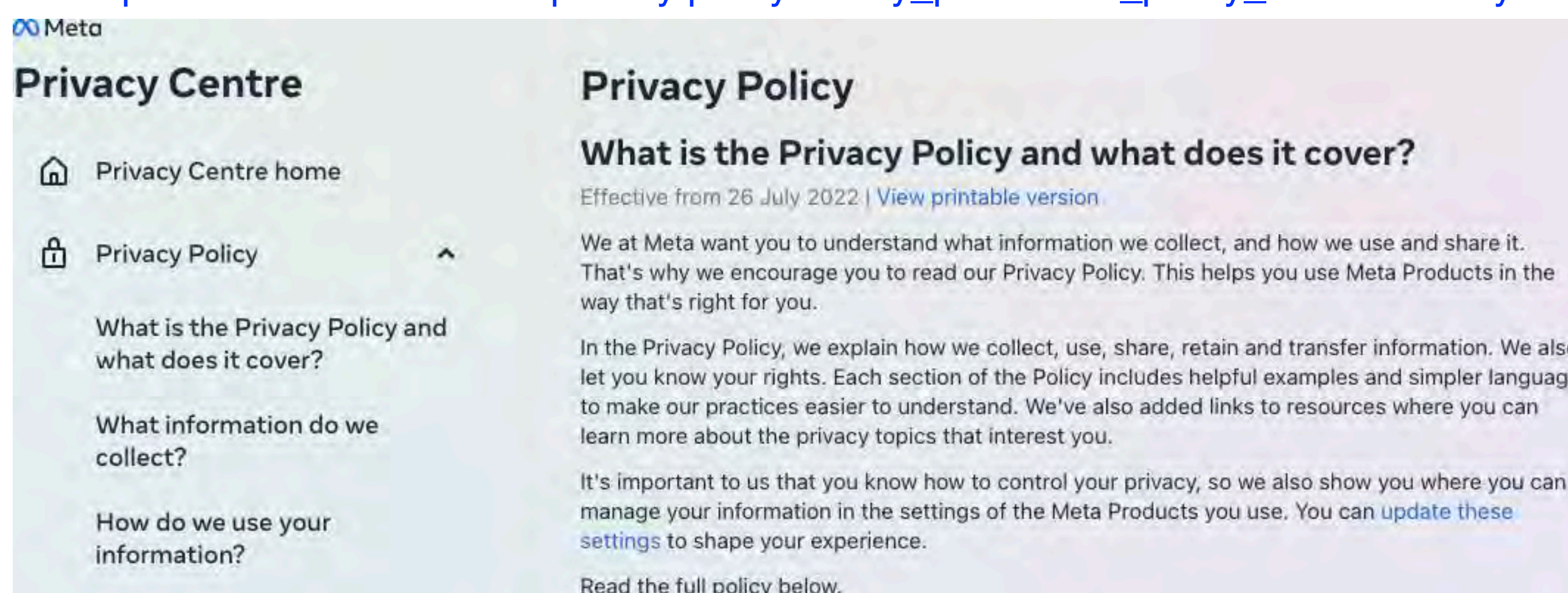
<https://policies.google.com/privacy?hl=en>

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

Facebook (Meta) & Privacy Shield

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

https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0



The screenshot shows the Facebook (Meta) Privacy Centre interface. On the left, the 'Privacy Centre' sidebar includes links to 'Privacy Centre home', 'Privacy Policy', and three expandable sections: 'What is the Privacy Policy and what does it cover?', 'What information do we collect?', and 'How do we use your information?'. The 'Privacy Policy' section is currently expanded. The main content area, titled 'Privacy Policy', contains the heading 'What is the Privacy Policy and what does it cover?' followed by text stating the policy is effective from 26 July 2022 and provides a link to a printable version. It explains that Meta wants users to understand information collection and usage, encourages reading the policy, and details how Meta explains collection, use, share, retain, and transfer of information, including user rights and links to resources. It also mentions that users can control their privacy through settings and provides a link to 'update these settings'. At the bottom, it says 'Read the full policy below.'

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

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

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.

Amazon.com Privacy Notice

1

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

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

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

EU-US and Swiss-US Privacy Shield

2

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


Amazon

EU-US and Swiss-US Privacy Shield


3

EU-US Privacy Shield Framework

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

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

If you have any inquiries or complaints about our handling of your personal information under Privacy Shield, or about our privacy practices generally, please contact us at: privacysield@amazon.com. 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 >](#)



Whatsapp



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

Binding corporate rules (BCR)

BCR

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

Procedure - art. 47(1)

Authority: The competent supervisory authority (Lead Authority)

Criterion: Consistency mechanism set out in Article 63

Conditions - art. 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 employees;
- (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.

Commission's Role - art. 47(3)

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).

Content of the BCRs - art. 47(2)

The binding corporate rules referred to in paragraph 1 shall specify at least:

- (a) the **structure and contact details** of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- (b) the **data transfers or set of transfers**, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- (c) their **legally binding nature**, both internally and externally;
- (d) the **application of the general data protection principles**, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- (e) the **rights of data subjects** in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
- (f) the **acceptance by the controller or processor** established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;
- (g) **how the information** on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph **is provided** to the data subjects in addition to Articles 13 and 14;
- (h) the **tasks of any data protection officer** designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
- (i) the **complaint procedures**;
- (j) the **mechanisms** within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;
- (k) the **mechanisms for reporting and recording changes** to the rules and reporting those changes to the supervisory authority;
- (l) the **cooperation mechanism** with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);
- (m) the **mechanisms for reporting to the competent supervisory authority any legal requirements** to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- (n) the **appropriate data protection training** to personnel having permanent or regular access to personal data.

Art. 29 WP Opinions on the BCR

Opinion	Title
WP 256 rev. 01 - 6/2/2018 - BCR for controller	Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules
WP 257 rev. 01 - 6/2/2018 - BCR for processor	Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules
WP263 rev.01 - 16/04/2018 - approval procedure for controllers and processors	Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors
WP264 del 19/04/2018 - application form for controller	Recommendation on the approval of the Controller Binding Corporate Rules form
WP265 del 19/04/2018 - application form for processor	Recommendation on the approval of the Processor Binding Corporate Rules form

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

Application form for processor WP265

Standard Application for Approval of Binding Corporate Rules

PART 1: APPLICANT INFORMATION

1. STRUCTURE AND CONTACT DETAILS OF 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 for which approval of the BCRs is sought:

BCR approved

Approved BCR by the EDPB -> on the institutional EDPB website

Approved BCR adopted pre-GDPR by the Garante -> on the institutional website

Derogations for specific situations

Transfers of personal data to third countries or international organisations

(139) The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, **in particular on the level of protection in third countries or international organisations**, and promoting cooperation of the supervisory authorities throughout the Union.

Transfers of personal data to third countries or international organisations

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. ... Member States should adopt such **exemptions** and derogations on general principles, the rights of the data subject, the controller and the processor, the **transfer of personal data to third countries or international organisations**, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply.

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](#)).

International cooperation for the protection of personal data

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

- (a) **develop international cooperation mechanisms** to facilitate the effective enforcement of legislation for the protection of personal data;
- (b) **provide international mutual assistance** in the enforcement of legislation for the protection of personal data, **including through notification, complaint referral, investigative assistance and information exchange**, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- (c) **engage relevant stakeholders** in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
- (d) **promote the exchange and documentation** of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Passenger Name Record (PNR)

Passengers Name Record (PNR)

European Commission

Passengers Name Record (PNR)

Europe

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

Italy

Attuazione della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29 aprile 2004. (18G00081)

The Italian Supervisory Authority

1. Parere su uno schema di decreto legislativo
2. WPPJ - Working Party on Police and Justice

Italy

Transfers of personal data to third countries or international organisations

From the Italian Supervisory Authority website

Transfer of personal data abroad

<https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero>

Resolution of July 21, 2022 - Initiative inspection activities are taken care of by the Office of the Supervisor, including by means of the Guardia di Finanza, limited to the period July-December 2022 - July 21, 2022 [9809072].



transfers of personal data based on Google's analytics in connection with the provisions of the June 9, 2022 measure.

Deliberazione del 21 luglio 2022 - Attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo luglio-dicembre 2022 - 21 luglio 2022 [9809072]



trasferimento di dati all'estero sulla base degli analytics di Google, in relazione a quanto disposto con il provvedimento del 9 giugno 2022.

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

Principles relating to processing of personal data
Cristina Radu

Rome, 30 September 2022



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 of 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 not observes 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, fair 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 need to be informed and, if the case, need 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 obligation 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 informing 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 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 include 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 liberties 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

Reference 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, instructing courses for the employees, the permanent monitoring and procedures for dealing with the requests of data subjects



7. Accountability

(ii) Demonstrate the compliance

Reference 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: informing 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 instruction 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 liberties 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 act 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.



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

**Data controller and data processor
Filippo Bianchini**

Rome, 30 September 2022



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

What we will talk about

Training of Lawyers on
EU Law relating to Data
Protection 2

Privacy roles

- The controller
- The processor
- The joint controller

Obligations and liability

- Regulatory obligations
- Responsibilities and their allocation

The agreements

- Data communication agreement
- Data processing agreement



#TRADATA2

Privacy roles

ARTICLE 29 DATA PROTECTION WORKING PARTY



00264/10/EN
WP 169

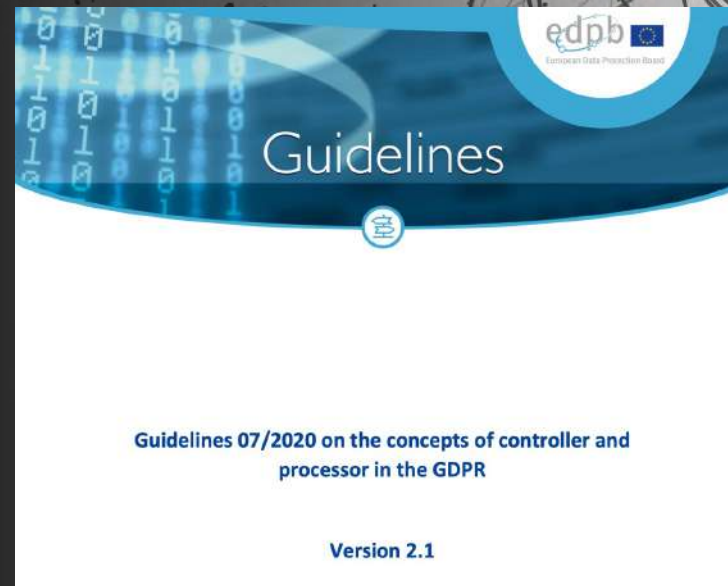
Opinion 1/2010 on the concepts of "controller" and "processor"

Adopted on 16 February 2010

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2



Data controller

The data controller

Training of Lawyers on
EU Law relating to Data
Protection 2

Definition

Purposes of the processing

Means of the processing

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

Responsibility of the organisation
as a whole

Ownership irrespective of contact
with the data



#TRADATA2

The data controller

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Identifying the data controller

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

Autonomous Ownership

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

Data processor

The data processor

Training of Lawyers on
EU Law relating to Data
Protection 2

Definition

Processor vs. appointee

Companies providing payroll services

"Irrelevant" processing

- Taxis and delivery
- Maintenance and cleaning

Controller's instructions

Excesses



#TRADATA2

The data processor

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

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2





Joint controller

The data processor

Training of Lawyers on
EU Law relating to Data
Protection 2



Definition



Shared Purposes and Means



Online advertising

Facebook fan pages and
use of Insight services
Fashion ID Case



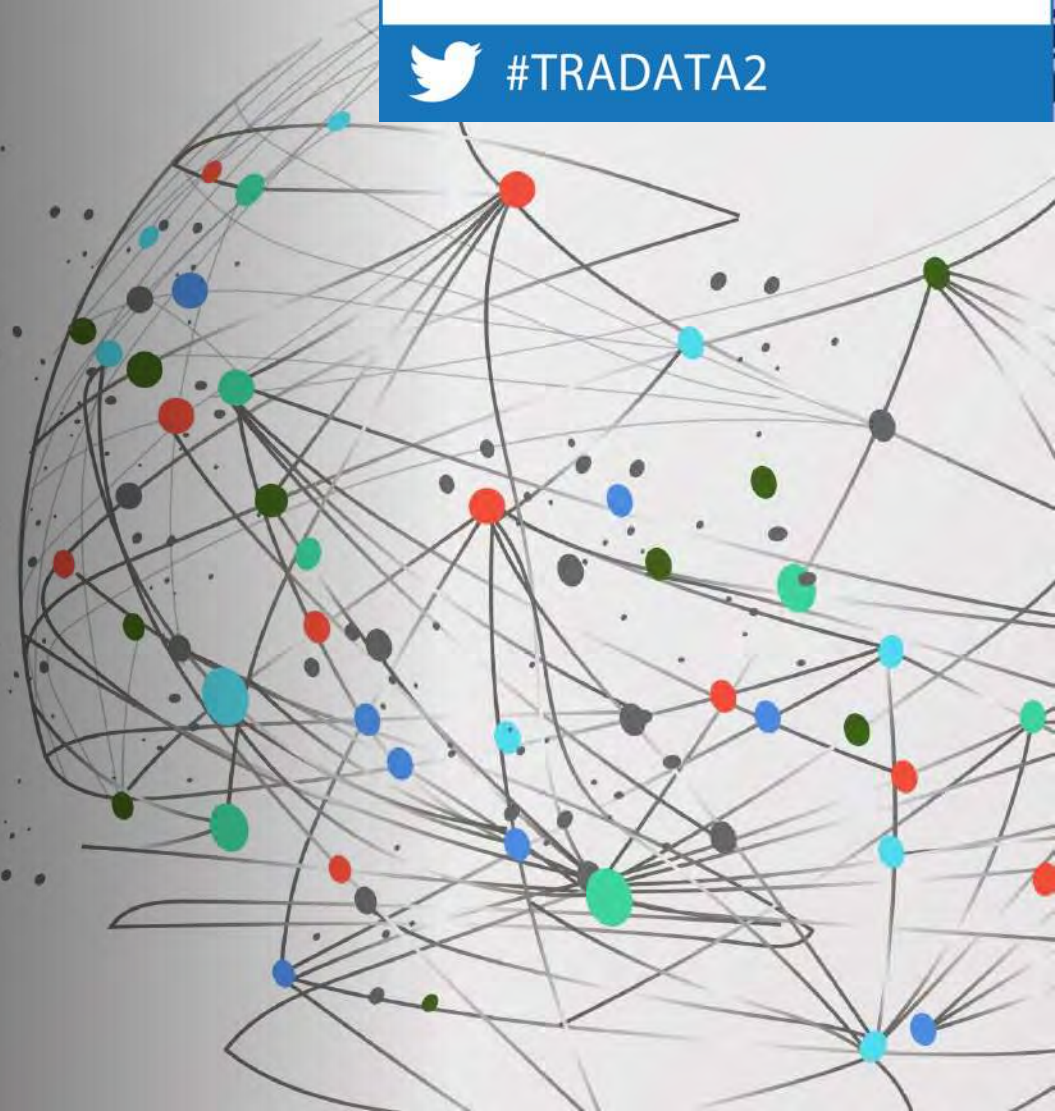
[The EDPB Guidelines on Social Media Targeting](#)



#TRADATA2



Obligations and liability





Regulatory obligations

Regulatory
obligations

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Obligations of the
data controller

Obligations of the
data processor



Responsibilities and their allocation

Responsibilities and their allocation

Training of Lawyers on
EU Law relating to Data
Protection 2



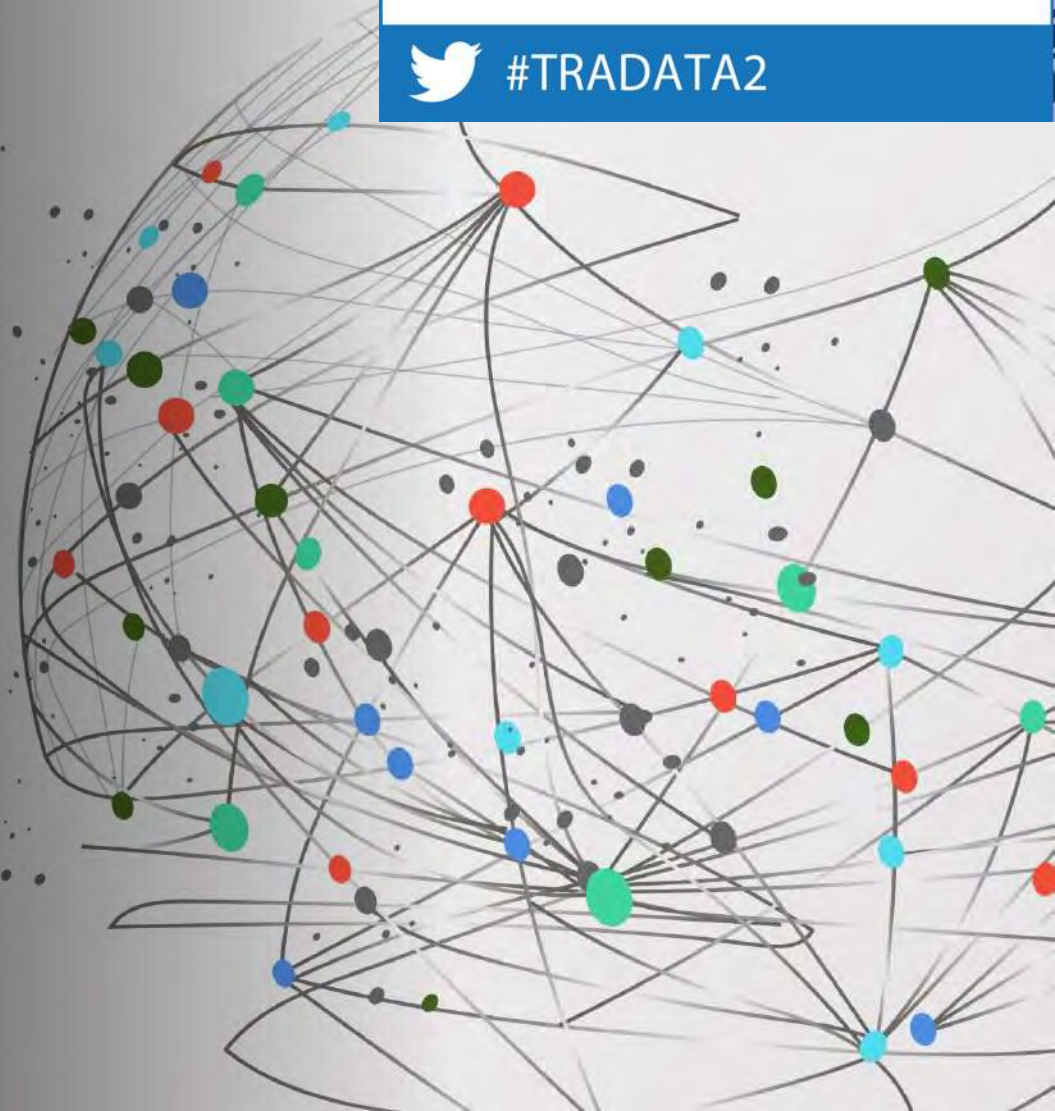
#TRADATA2

Joint and several liability
(Art. 82)

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



The agreements





Data Communication Agreements



Data Processing Agreement

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Data Processing Agreements (DPA)

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Preliminary verification

- Due diligence

Written authorisation

Minimum statutory content

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

Negotiating autonomy

Future
challenges

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Blockchain

Web3

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

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

Giovanni Battista Gallus

Rome, 30 September 2022



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

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

Training of Lawyers on



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

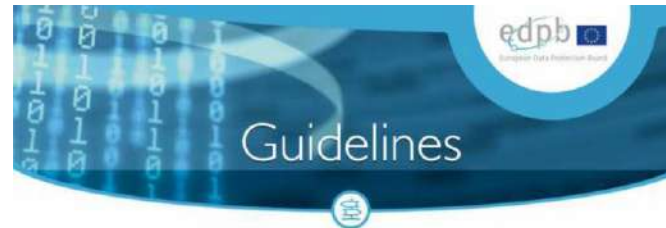
#MADATA2



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

Version 1.0

Adopted on 18 January 2022



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

Version 2.0

Adopted on 7 July 2020



Guidelines on the right to data portability

Adopted on 23 December 2016
As last Revised and Adopted on 8 April 2017

Useful guidelines

Training of Lawyers on EU Law relating to Data Protection 2



#TRADATA2



Common principles

Data Subject rights - definitions

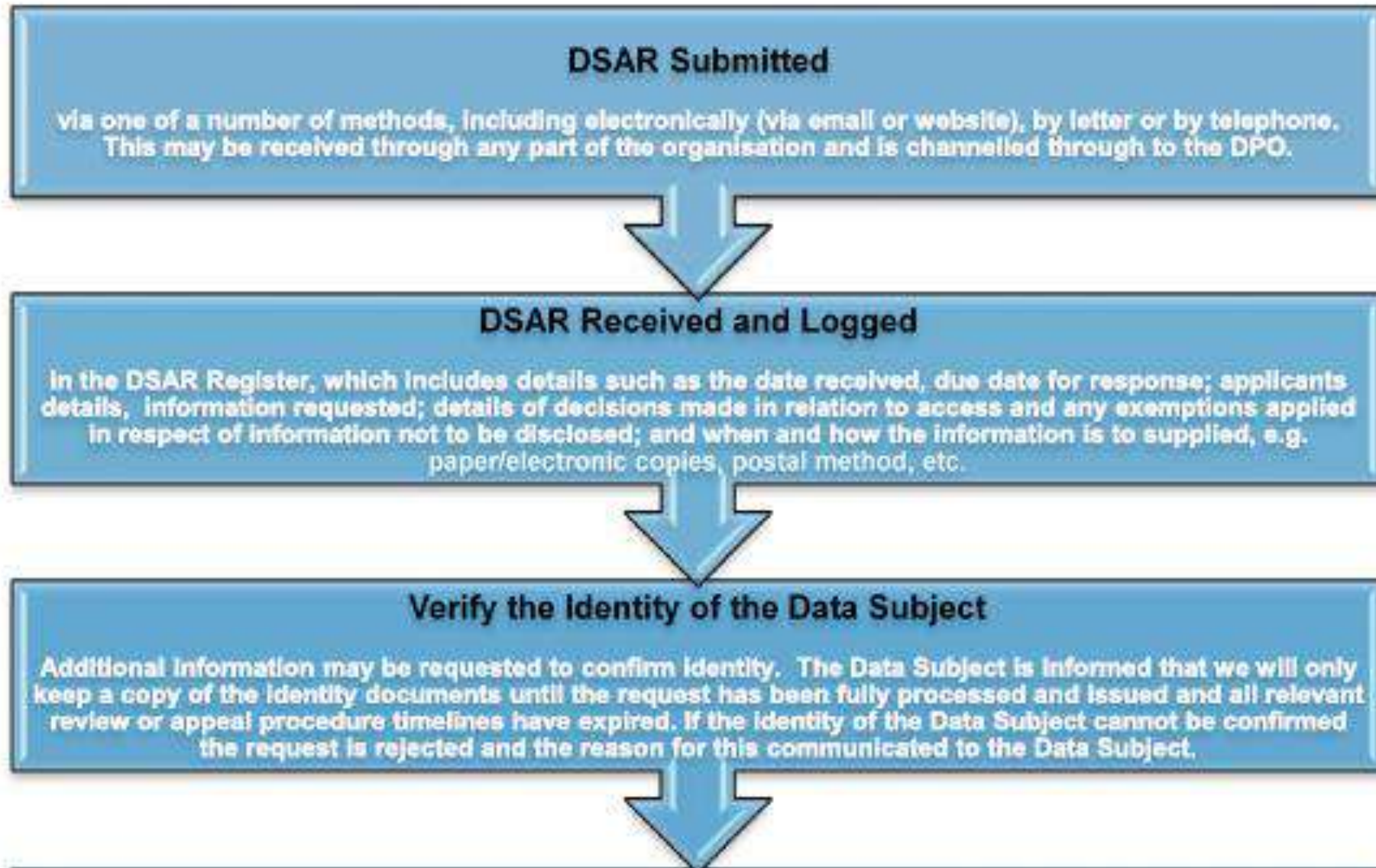
We all know the
definition of
Personal data...



We all know
who the Data
subject is...

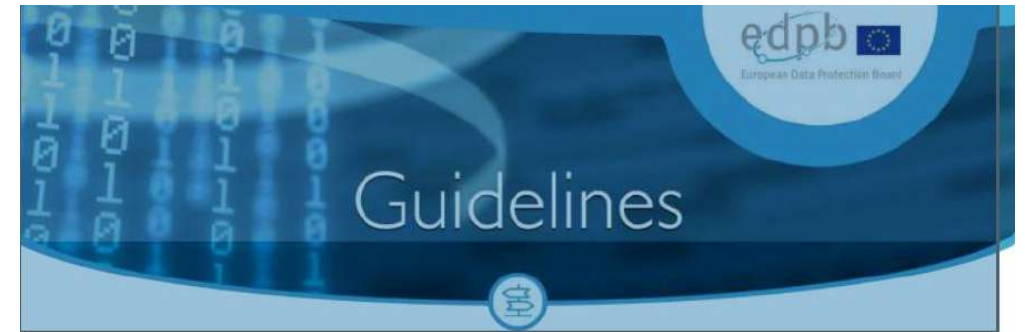
Training of Lawyers on
EU Law relating to Data
Protection 2

ADATA2



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

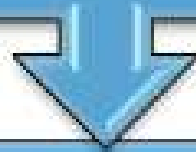
Version 1.0

Adopted on 18 January 2022



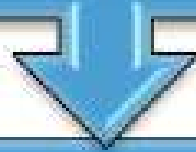
Evaluate Validity of Information Provided

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



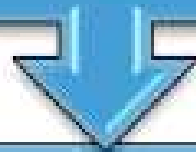
Identify and Compile the Personal Data

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



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 \(GDPR\)](#) ¹⁸ 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
- ...

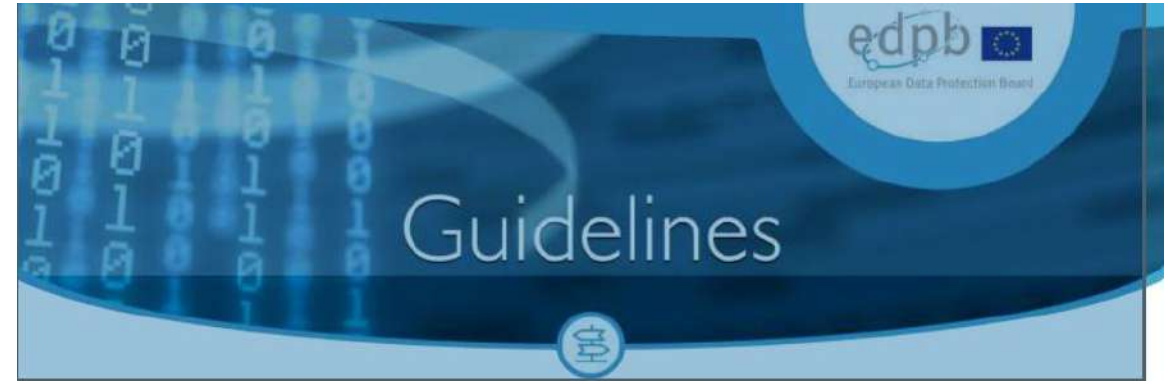
Focus on the right of access

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 1.0

Adopted on 18 January 2022

The right of access under the GDPR vs other access rights

Access to
public
documentation

FOIA requests

Does the request need a specific format?



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

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

 20 September 2022 

Background information

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



Summary of the Decision

Latest news

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

 23 September 2022 

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

 20 September 2022 

[September plenary - adopted documents](#)

 20 September 2022 

[New EDPB opinion on certification criteria](#)

The right of access – overall aim



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



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

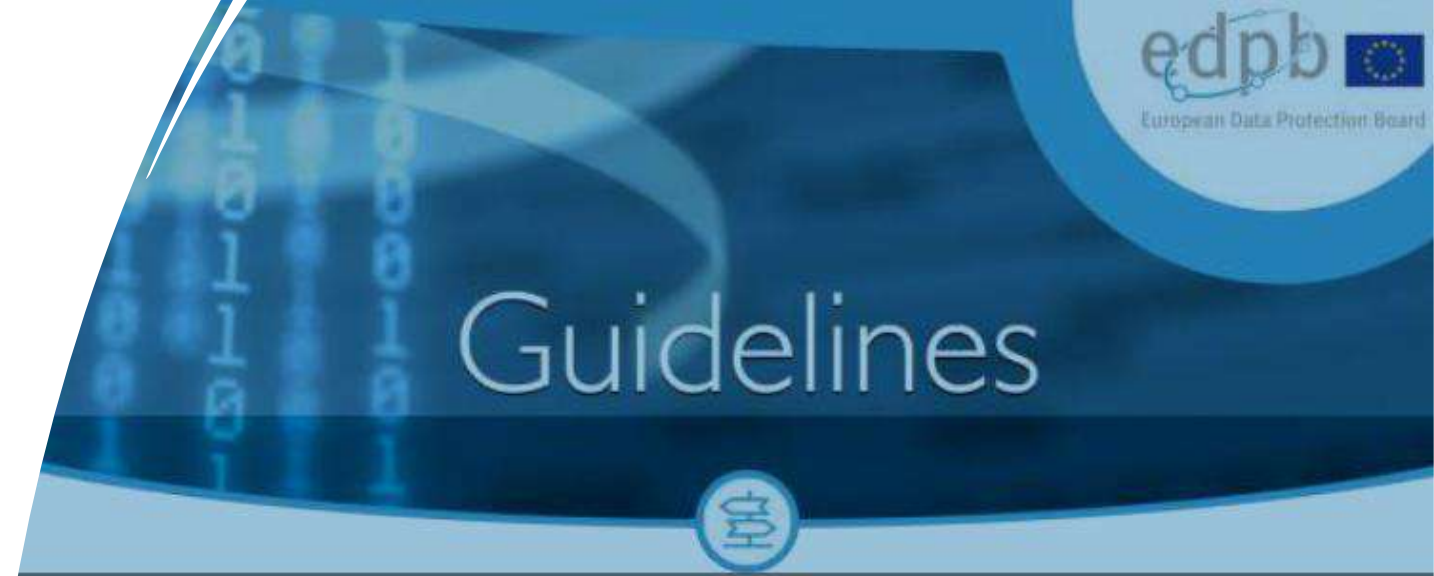
The right of access

three different components:

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

Access to this personal data and

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



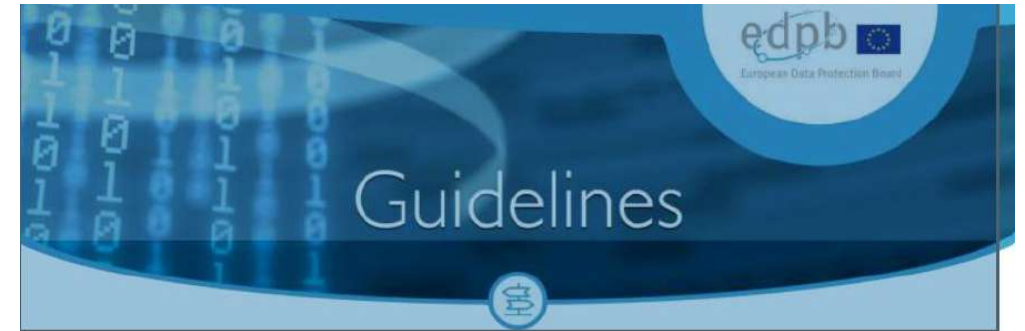
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

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

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



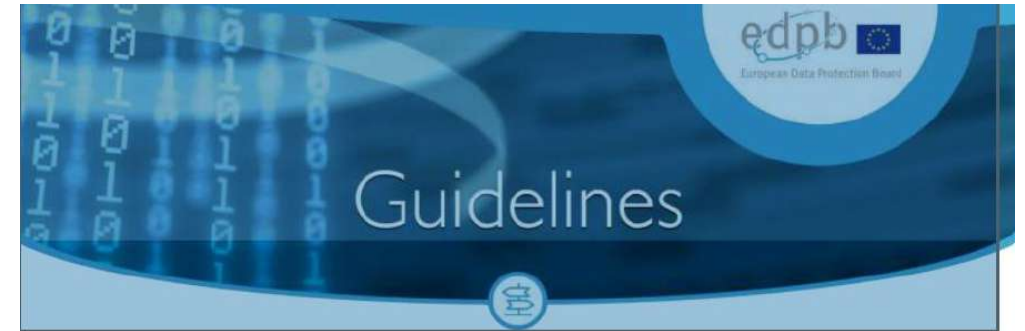
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Which data?

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



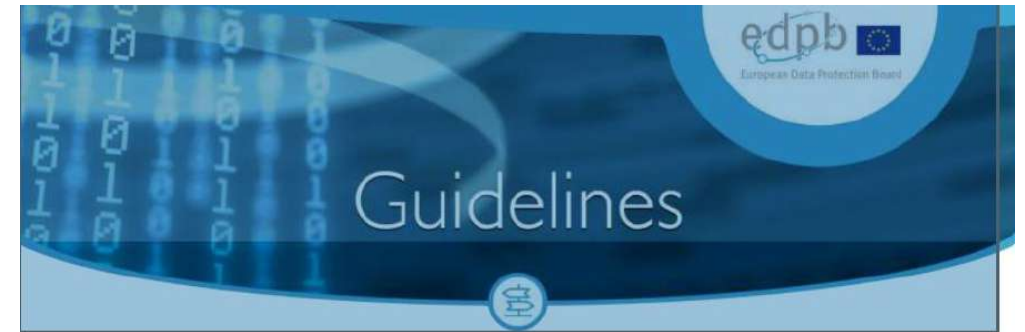
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Does it include inferred data?

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



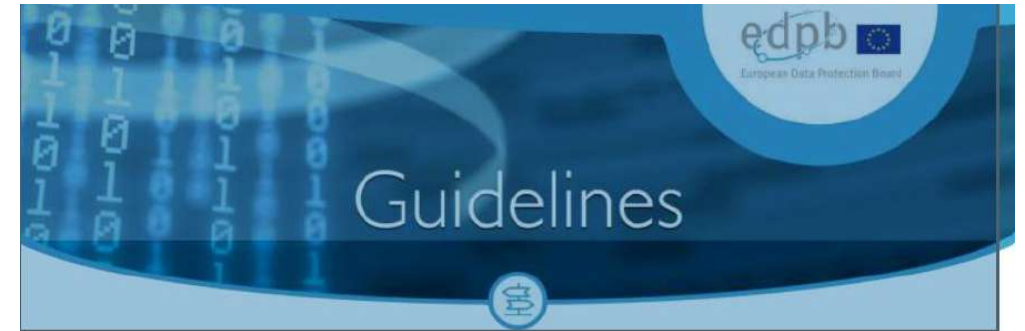
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Limits and restrictions

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



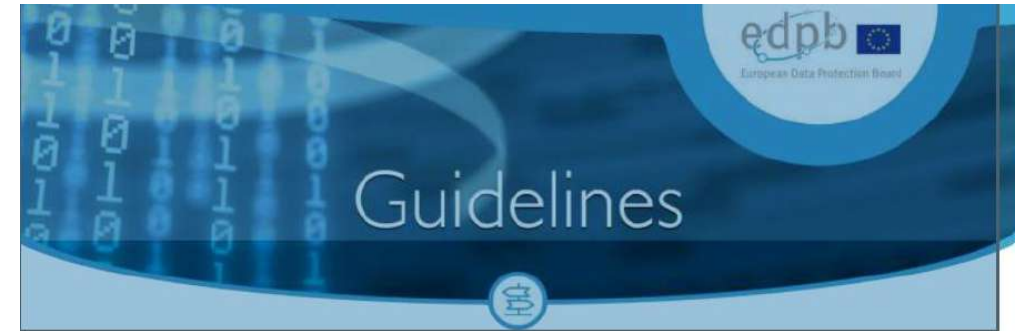
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Security!

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



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

Version 1.0

Adopted on 18 January 2022

Can DSR become a threat?

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

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

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

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

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

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

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

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

This paper makes the following contributions:

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

Blackhat USA 2019 Whitepaper

James Pavur and Casey Knerr

GDPArrrrr: Using Privacy Laws to Steal Identities

James Pavur*
DPhil Researcher
Oxford University

Casey Knerr
Security Consultant
Dionach LTD

DSR and law enforcement directive

DSR & Directive 2016/680

ARTICLE 29 DATA PROTECTION WORKING PARTY



17/EN

WP 258

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

Adopted on 29 November 2017

Recommendations of the WP29

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

DSR & EUROPOL REGULATION



EUROPEAN DATA PROTECTION SUPERVISOR

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

Search the site

EDRi

About us What we do Take action

Home » Resources » Rather delete than comply: how Europol snubbed data subject rights

Rather delete than comply: how Europol snubbed data subject rights

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

By EDRi | September 28, 2022

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

Enhanced portability?

Digital Markets Act (applies to the Gatekeepers)

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

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

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

Interplay between data protection and human
rights: how to ensure a fruitful interaction
among fundamental rights

Luigi Montuori

Rome, 30 September 2022



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

HOW TO ENSURE A FRUITFUL INTERACTION AMONG FUNDAMENTAL RIGHTS

Training of Lawyers on
EU Law relating to Data
Protection 2

Complementarity of rights vs. Conflict' of rights



#TRADATA2

New technologies may impact many fundamental rights at the same time, including, but not limited to, **data protection and privacy**, non-discrimination and access to an effective remedy.

Data protection, with the **GDPR** in place, has a strong legal framework in the EU.



Data protection principles can also help address other fundamental rights, such as non-discrimination and access to an effective remedy:

- when privacy acts as enabling right for the enjoyment of other rights, in particular the free development and expression of an individual's personality, and the non-discrimination;
- when it gets in conflict with other fundamental rights, thereby requesting an appropriate balancing of rights;
- when data protection is called upon to play a role in the absence of other specific rights.



In the construction of new policies there is a need for new tools of protection in particular the introduction of **human rights impact assessment**, with the involvement of DPA, and participatory models;

Privacy is an enabling right but it needs enabling conditions (e.g. equal access to digital services, literacy) as **privacy is not and should not be a privilege for few**. It is a fundamental component of social justice;

Data protection cannot become the “**law for everything**”: specific new tools should be provided when necessary for the protection of new challenges for human rights.

There is a tendency to “use” data protection in the absence of other forms of protection. Is data protection a solution for all?



- The very fact that the EU and the Council of Europe are working on legislation on artificial intelligence (AI) shows that data protection law is not a solution for everything, and further safeguards are needed to protect fundamental rights in relation to new technologies. In addition, the recently adopted **Digital Services Act** addresses several fundamental rights risks in relation to the use of online services.



The **GDPR requires impact assessments** in relation to other fundamental rights as well, which can be used to also safeguard other rights. When assessing the risks of personal data processing, unfair treatment also needs to be considered.

- At the same time, data protection may be seen in conflict with safeguarding other rights. Assessing discrimination may require collecting sensitive data on protected characteristics, which is not easily possible.
- On facial recognition technologies the limitation of the right to privacy and data protection has to follow a strict procedure and test, and can only be if necessary and proportionate.
- The right to data protection may also be limited, as it is not an absolute right.



The relevant political discussion:

- Article 10 (5) of the **Artificial Intelligence Act** (Proposal) explicitly mentions bias monitoring, detection and correction as a separate justification for the processing of sensitive categories of personal data. Such data could only be collected when strictly necessary. This means that those collecting data have to be able to prove that **they cannot detect, monitor or mitigate potential discrimination with available data**;
- the recently adopted **Digital Services Act** addresses several fundamental rights risks in relation to the use of online services.

Virtuous examples: when privacy is instrumental to the enjoyment of other rights (including non discrimination).

Data protection may be seen as the entry point to also safeguard other fundamental rights, most notably because it is well established law when it comes to the use of new technologies.

There are a few examples in relation to **court decisions** about algorithms and new technologies, where data protection and privacy are used to stop the use of the systems, which likely also safeguards other rights.

In the Netherlands, the so-called ‘System Risk Indication’ was developed as a government tool to alert the Dutch public administration about fraud risk of citizens, by processing and linking large amounts of their personal data from public authorities. The court ruled that SyRI impinges is proportionately on the private life of citizens. The court found that everyone whose data was analysed by SyRI was exposed to this risk. In addition, due to the opacity of the algorithm used, citizens could “neither anticipate the intrusion into their private life nor can they guard themselves against it.” The ruling of 5 February 2020 (in Dutch) is available online.

- UK Court of Appeal: police use of facial recognition violates human rights: a first instance decision of the Divisional Court of Cardiff in 2019 dismissed a claim concerning the lawfulness of the South Wales Police’s use of the “AFR Locate” face recognition system. The Court of Appeal overturned that decision.

Garante, Foodinho's management violated Article 22(3) of the GDPR
"Riders: Italian SA says no to algorithms causing discrimination, a
platform in the Glovo group fined EUR 2.6 million" [Rider: Garante](#)
[privacy, no a discriminazioni basate sugli algoritmi.... - Garante Privacy](#)



#TRADATA2

Another example is a fine by GARANTE:

Fines Foodinho Over Its Use of Performance Management Algorithms. The authority held Foodinho in breach of the principles of transparency, security, privacy by default and by design, and held it responsible for not implementing suitable measures to safeguard its employees' (i.e., riders') rights and freedoms against discriminatory automated decision making. The Garante's decision is the first of its kind in the realm of the algorithmic management of gig workers.

Future challenges

The role of supervisory authorities.



Users of AI are not always clear which supervisory authority is responsible when it comes to algorithms.

Independent oversight, with sufficient resources, is crucial for safeguarding fundamental rights.

How far should they go while assessing the impact of processing?

Shouldn't the assessment concern the whole “human rights package” or be limited to the data protection aspects only?

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

Consent under the GDPR
Vincenzo Colarocco

Rome, 30 September 2022



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

Vincenzo Colarocco, Att.

*Studio Previti Law Firm– Head
of "Compliance, media and
technology" department*



Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Areas of activity

- Data protection
- IT and Legal Tech
- Cybersecurity
- Innovation
- Web and corporate reputation
- Communication law
- Compliance
- Intellectual Property

What we do

- Strategic consulting
- Preparation and legal and contractual negotiation
- Management of all GDPR compliances

Table of contents

Definition of consent (3)

Elements of Valid Consent (4 – 8)

Nature of Consent: Italian and European Jurisprudential Focus (9)

Decisions on The Nature of Consent (10 – 17)

Children's Consent and parental responsibility: Jurisprudential Focus (18 – 20)

Marketing and Consent: Italian Jurisprudential Focus (21 – 23)

Conclusions (24)

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Definition of consent under GDPR and its application in Italy

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



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

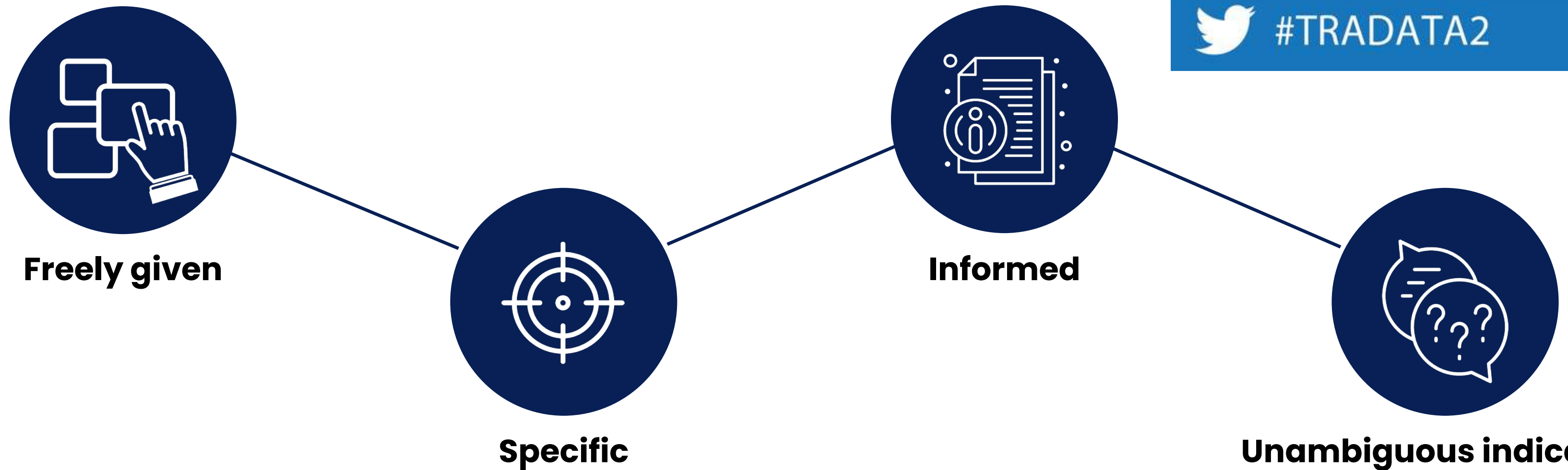
Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2



Elements of valid consent



Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

Unambiguous indication
of the data subject's wishes by
which he or she, by a statement
or by a clear affirmative action,
signifies agreement to the
processing of personal data
relating to him or her.

Elements of valid consent

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



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 unknow

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

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 dissemination. 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

The matter

A company had developed a method for rating and reviewing people, especially professionals. Specifically, the web platform and its computer archive was aimed at developing the reputational profiles of natural persons and legal entities, against the phenomenon of creating artificial or untrue profiles, through 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>)

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,
Sez. 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

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.



Active behaviour of the data subject

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

The data controller has to be able to demonstrate that the data subject, by means of active conduct, has given his consent to the processing of his personal data, after having first obtained the privacy policy. Specifically, the Court censures the method of acquiring consent by means of a pre-selected tick box, because that activity does not imply active conduct on the part of a website user.

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.



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.

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).

Children's Consent and parental responsibility

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 the provision of information society services directly to a child, 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 responsibility

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 Tik Tok **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 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 been long 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 jurisprudential focus

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2

OVERVIEW OF DECISIONS ON ACQUIRING AND WITHDRAWING CONSENT

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

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 the disclosure of data 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

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.

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 in ***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, but represents the ***fundamental way*** to protect ***freedoms*** and ***rights of the data subject***, as the broadest expression of the principle of individual self-determination.

Training of Lawyers on
EU Law relating to Data
Protection 2



#TRADATA2