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

General data protection regulation introduction

Elena Spiropoulou

Athens, 23 June 2023

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

THE HISTORY OF THE GENERAL DATA PROTECTION REGULATION

1995 Directive 95/46/EC is adopted

The European Data Protection Directive (Directive 95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is adopted.

It was integrated in all countries legislation, as internal law with slight differences.

THE HISTORY OF THE GENERAL DATA PROTECTION REGULATION

January 2012 **EC proposal to strengthen online privacy rights and digital economy**

- The European Commission proposes a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy.

March 2012 **WP29 Opinion on data protection reform proposal**

- The Article 29 Working Party adopts an Opinion on the data protection reform proposal.

THE HISTORY OF THE GENERAL DATA PROTECTION REGULATION

May 2016 The Regulation enters into force, 20 days after publication in the Official Journal of the EU

May 2018 Implementation by all countries

THE GDPR APPLIES TO:

- Personal Data of Natural persons, not entities
- Alive persons, not deceased.
- Avtivities that fall outside of purely household activities
- Controllers or Processors based within the EU
- Personal data of EU subjects even if the Controller or Processor is outside the EU, as long as it concerns offering of goods and services or monitoring of EU subjects' behavior.

DEFINITIONS

- Personal data: any information relating to an identified or identifiable natural person (‘data subject’); identifiable natural person = can be identified, directly or indirectly, by reference to an identifier (name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- Special Categories: reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data data concerning health or data concerning a natural person's sex life or sexual orientation

DEFINITIONS

- Processing: any operation performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- Profiling: any form of automated processing of personal data aiming to evaluate personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
- Pseudonimization: no longer be attributed to a specific data subject without the use of additional information
- Filing system: structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis

DEFINITIONS

- CONTROLLER/JOINT CONTROLLERS: natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
- PROCESSOR: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
- RECIPIENT: natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not
- THIRD PARTY: other than the Controller, theProcessor (or acting on behalf of them) or the Data subject.

PRINCIPLES PERSONAL DATA MUST BE PROCESSED:

- lawfully fairly and in a transparent manner in relation to the data subject
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (minimisation)
- accurate and, where necessary, kept up to date (accuracy)
- no longer kept than necessary (storage limitation)
- Integrity and confidentiality
- Accountability

LEGAL BASES OF PROCESSING ARTICLE 6

- Consent
- performance of a contract to which the data subject is party / in order to take steps at the request of the data subject prior to entering into a contract
- compliance with a legal obligation to which the controller is subject
- Protection of the vital interests of the data subject or of another natural person;
- performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

Is it a lawful process if we process personal data collected for a specific purpose for another purpose?

We have to consider:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing

- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller

- the nature of the personal data, in particular whether special categories of personal data are processed

- the possible consequences of the intended further processing for data subjects

- the existence of appropriate safeguards, which may include encryption or pseudonymisation

LEGAL BASES OF PROCESSING ARTICLE 9

- Processing of Special Categories' Personal Data is prohbited unless:

- Consent for a specified purpose
- Employment laws and social security/social protection laws
- Vital interests od a DS or third party unable to consent
- legitimate activities of a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members /former members
- manifestly made public by the data subject

LEGAL BASES OF PROCESSING ARTICLE 9

- processing is necessary for reasons of substantial public interest,
- preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- public interest in the area of public health
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)
- Processing by HCPs

RIGHTS OF THE DATA SUBJECT

- Information (about the Controller, purpose, recipients, legal basis, data processed, time etc)
- Right of access
- Right to rectification
- Right to erasure (“Right to be forgotten”)
- Restrictoin of processing
- Data portability
- Right to object
- Right not to be subject to a decision based solely on automated processing including profiling, which produces legal effects to the DS

CONTROLLER'S RESPONSIBILITIES:

DATA PROTECTION BY DESIGN AND BY DEFAULT

- appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
- technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. (amount of, extend, time, accessibility)

PROCESSOR'S RESPONSIBILITIES

- Acting on behalf and within the orders of the Controller
- Confidentiality agreements
- Technical and organizational measures for the protection of personal data
- Deletes or returns personal data
- Not to hire subprocessor without the permission of the Controller
- Assist controller in compliance

CONTROLLER & PROCESSOR'S RESPONSIBILITIES

- Cooperation with the Supervising Authority
- Keeping records of any processing.
- Security of processing
- Notification of a pd breach to the supervising authority
- Communication of a data breach to the data subject

DATA PRIVACY IMPACT ASSESSMENT

It is necessary to assess the risk of processing when

- systematic and extensive evaluation of personal aspects is taking place based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
- processing on a large scale of special categories of data or
- systematic monitoring of a publicly accessible area on a large scale

DATA PRIVACY IMPACT ASSESSMENT

- systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller
- assessment of the necessity and proportionality of the processing operations in relation to the purposes
- assessment of the risks to the rights and freedoms of data subjects
- measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned

DATA PROTECTION OFFICER

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- core activities of the controller or the processor consist of processing on a large scale of special categories of data

DATA PROTECTION OFFICER

- inform and advise the controller or the processor and the employees who carry out processing of their obligations
- monitor compliance with this Regulation
- provide advice where requested as regards the data protection impact assessment and monitor its performance
- cooperate with the supervisory authority
- act as the contact point for the supervisory authority on issues relating to processing,

TRANSFER OF DATA

- Free transfer of personal data within the EU
- As well as to countries covered by adequate decision (Andora, Argentina, Canada, Faroe Islands, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, UK, Urugay, Republic of Korea, Guernsey)
- Contractual Clauses
- Approved Corporate binding rules

PENALTIES

- FINES UP TO 10.000.000 euros or 2% of global annual turnover
- FINES UP TO 20.000.000 euros or 4% of global annual turnover
  - breach of basic principles
  - data subjects' rights
  - rules for transfer of data

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

The rights of data subjects, including rights during investigations and criminal proceedings

Florence Ivanier

Athens, 23 June 2023

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

Summary: Rights of data subjects including in investigations and criminal proceedings

1) Applicable sources of law
   - ✓ European data protection package: GDPR & Law Enforcement Directive
   - ✓ Directive Passenger Name Record (PNR)
   - ✓ Respective scopes of application of GDPR & LED
2) What rights and what content under GDPR ?
   - ✓ Focus : the right of access and the rise of its instrumentalization
3) Limits to data subjects' rights under the LED

1) Applicable sources of law

GDPR

EU Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016

=> directly applicable in member States since May 25, 2018

- Section 1 - art. 12 - Transparency of information and communications and procedures for exercising rights
- Section 2 - Information and access to personal data (art. 13 to 15)
- Section 3 - Rectification and erasure (art. 16 to 20)
- Section 4 - Right of opposition and automated individual decision (art. 21-22)
- Section 5 - Limitations - art. 23

1) Applicable sources of law

Law Enforcement Directive

DIRECTIVE (EU) 2016/680 of April 27, 2016, on the protection of individuals with regard to the processing of personal data (…) for the purposes of crime prevention and detection, investigations and prosecutions in this matter, or the enforcement of criminal sanctions (…)

- Chapter 3: Rights of the data subject: Article 12 to 18 of the Directive

1) Applicable sources of law

Directive on the use of Passenger Name Record (PNR)

May 25, 2018

Data for the prevention and detection of terrorist offenses and serious crime, as well as for investigations and prosecutions

Limitations:

- prohibits the collection and use of sensitive data
- PNR data can only be kept for a period of 5 years, and must be depersonalised after a period of 6 months so the data subject is no longer immediately identifiable
- Member States establish a passenger information unit to handle and protect the data
- automated processing of PNR data cannot be the only basis for decisions producing adverse legal effects

1) Respective scopes of LED & GDPR

Law Enforcement Directive - 2 cumulative conditions

a) The purpose is the prevention and detection of criminal offenses or investigations and prosecutions, or the execution of criminal sanctions, including protection against threats to public security (...)

i. In criminal matters: prevention and detection of offenses related to passenger travel (API-PNR processing) or management of measures related to judicial penalties enforcement

ii. Activities not falling within the criminal sphere but related to police activities conducted prior to the offense, such as protection against threats to public security and maintaining public order.

b) processing is carried out by a competent authority

i. which includes any public authority competent for the prevention and detection of criminal offenses, prosecutions, or the execution of criminal sanctions, such as judicial authorities, police, and law enforcement agencies

ii. any other organization entrusted with the exercise of public authority and public power for the purpose of implementing a processing covered by the LED, such as sports federations for the security of sporting events, etc.

GDPR covers data processing falling within the scope of EU law in both public & private sectors

aurele IT avocats

2) What data subjects' rights under GDPR?

- ❑ Right to be informed
- ❑ Right of access (15)
- ❑ Right to rectification (16)
- ❑ Right to erasure - to be forgotten (17)
- ❑ Right to restrict processing (18)
- ❑ Right to know about recipients (19.2)
- ❑ Right to data portability (20)
- ❑ Right to object to processing (21)
- ❑ Right not to be subject to an automated decision, including profiling (22)
- ❑ Right to withdraw consent (7.3)
- ❑ Right to be informed of a data breach (34.1)
- ❑ Right to lodge a complaint with a supervisory authority (77.1) and right to an effective judicial remedy against a supervisory authority (78)
- ❑ Right to obtain compensation for damages (82.1)

2) What data subjects' rights under GDPR? Focus on the right of access (15)

Right to :

- ✓ confirmation as to whether data are being processed
- ✓ access to the data and to information on:
  - purpose
  - categories
  - recipients
  - retention
  - rights
  - where the data are not collected from the data subject, information as to their source
  - automated decision making

Focus on the right of access

- Which data?
  - any data pertaining to the data subject
  - regardless of the medium used: paper, audio recording, video, stored in current databases or intermediate archives
- What is the response time?
  - response within one month (8 days for health data)
- In what form?
  - concise, transparent, understandable, and easily accessible form.
- At what cost?
  - free of charge, subject to the limits specified below

Focus on the right of access

What limitations?

- Respect for the rights and freedoms of others: not infringing on the rights of third parties

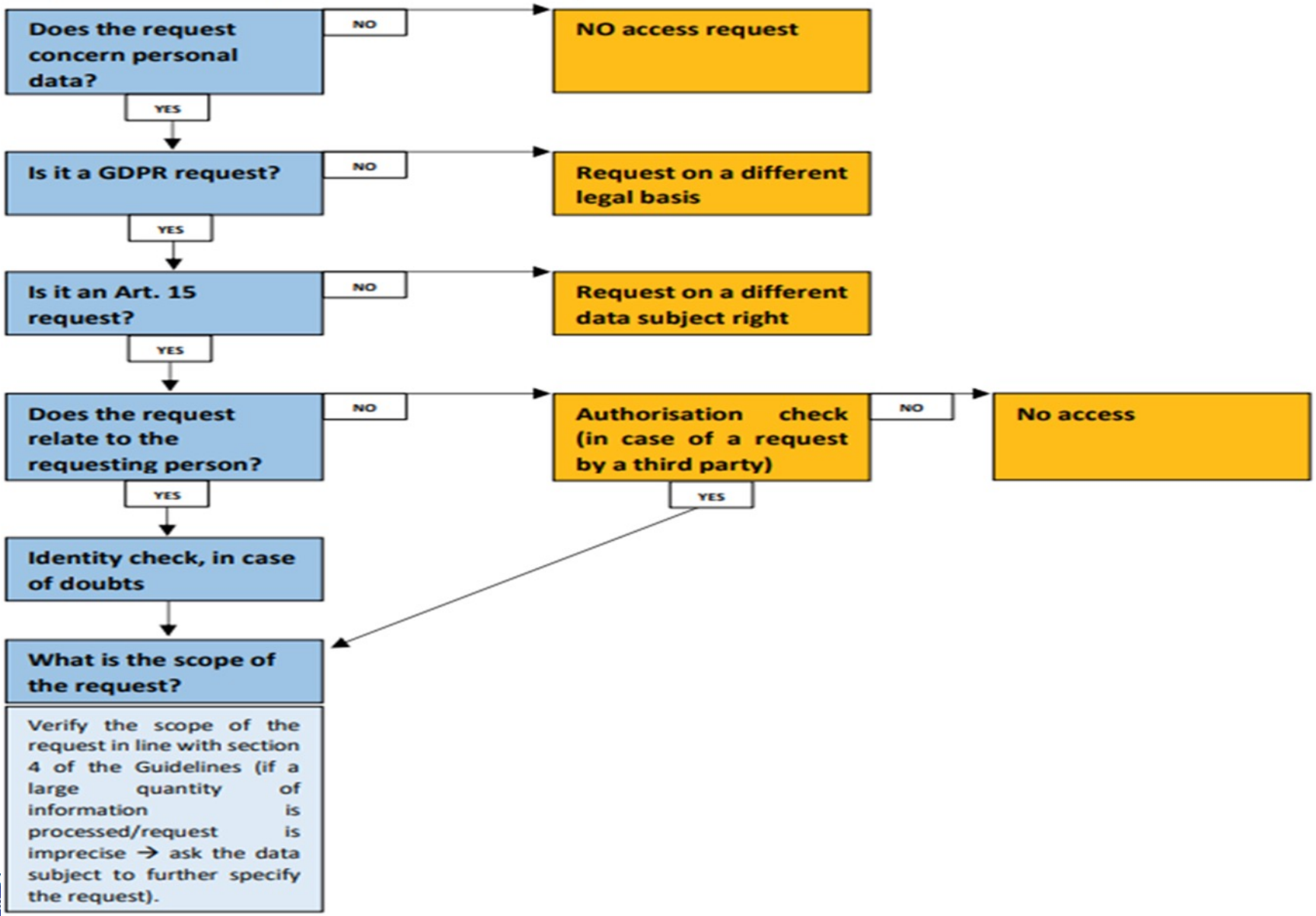
  => In practice, elements that could identify a third party, infringe on the secrecy of correspondence, privacy, or trade secrets must be removed

- Manifestly unfounded or excessive requests (including repetitive nature), the controller may:

  a) demand reasonable fees considering the administrative costs incurred

  b) or refuse to comply with such requests

Step 1: How to interpret and assess the request?



aurele IT
avocats

The right of access and the rise of its instrumentalization

An emblematic and almost unlimited right that fulfills the objective of the GDPR to enhance individuals' control over their data.

⇒ However, it is now widely misused for contentious purposes:

⇒ labor disputes, commercial conflicts, or consumer cases, aiming to obtain broad access to data for purposes other than verifying the processing of personal data

⇒ This misuse allows circumventing civil procedure in order to obtain evidences in trials and for retaliatory actions.

The question has been settled:

⇒ The right of access is unconditional and does not require justification based on a legitimate motive (EDPB guidelines March 28, 2023: "*data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Article 15 GDPR are met, the purposes behind the request should be regarded as irrelevant.*"

Right of rectification (18)

=> right to obtain from the controller without undue delay the rectification of inaccurate data or to have incomplete data completed

Right to restriction of processing (18)

Which scope of application?

4 cases of limitation:

(a) the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead

(c) the controller no longer needs the data for the purposes of the processing, but they are required by the data subject for the establishment or defence of legal claims

(d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject

Right to data portability (20)

Where:

- the processing is based on consent or contract
- the processing is automated (as opposed to processing on paper or manual)

=> The data subject has the right to:

- receive the data concerning him or her in a structured, commonly used and machine-readable format
- to transmit those data to another controller without hindrance

Limitations

- not applicable in case of public interest or exercise of official authority entrusted to the controller.
- the right to data portability must not adversely affect the rights and freedoms of others

LED: specific controller's obligations

- Consult the supervisory authority if the Data Protection Impact Assessment (DPIA) presents high residual risks or if the processing, due to the use of new mechanisms, technologies, or procedures, presents high initial risks.
- Establish a clear distinction between personal data of different categories of data subjects (LED art. 6)

  => For example, individuals convicted of a criminal offense, victims, and third parties.
- Differentiate between personal data based on facts and those based on personal assessments (LED art. 7)
- Process sensitive data only in cases of absolute necessity (LED art. 10)

Data subjects' rights under the LED

❖ Rights not included: right to data portability

❖Rights limited under the LED

✓ Right of access - limitations to avoid hindering investigations, preventing and detecting criminal offenses.

=> In practice, the limitation of the right of access may result in the implementation of an indirect right of access, exercised through the supervisory authority.

✓ Right to limitation - 2 hypotheses only:

(i) data kept for purposes of evidence in a litigation or

(ii) If it cannot be determined whether the data is accurate or not

Thank you for your attention

Florence Ivanier
Attorney – DPO
fivanier@aurele-it.fr
www.aurele-it.fr
6, rue Jean de Lafontaine 75016 Paris
+ 33 1 89 16 81 12

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

Data controller and processor

Iliana Kosti

Athens, 23 June 2023

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

DEFINITIONS (A. 4 OF THE GDPR)

- ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

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

WHY ARE DEFINITIONS IMPORTANT?

- 1. The role of the parties in data processing defines the parties' responsibilities
- 2. The exercise of the data subjects' rights depends on the roles of the parties
- 3. Accountability a. 5(2) as the main principle of the GDPR: **the controller** shall be responsible for implementing appropriate technical and organizational measures and be able to demonstrate compliance with the principles set out in a. 5(1).
- 4. Both controllers and processors:-can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them and are directly accountable towards supervisory authorities by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders (a. 58 GDPR).

CONTROLLER: "A NATURAL OR LEGAL PERSON, PUBLIC AUTHORITY, AGENCY OR OTHER BODY"

(E. VAGENA, TRADATA 2, 2022)

- -No limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.
- -In practice, however, it is usually the organization as such, and not an individual within the organization (such as the CEO, an employee or a member of the board), that acts as a controller
- -Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller
- -In principle, any processing of personal data by employees which takes place within the realm of activities of an organization may be presumed to take place under that organisation's control. In exceptional circumstances, however, it may occur that an employee decides to use personal data for his or her own purposes, thereby unlawfully exceeding the authority that he or she was given. (e.g. to set up his own company or similar)*EDPB,Guidelines on the Concepts of Controller, Processor and Joint Controllership Under Regulation (EU) 2018/1725(2019).

THE CONTROLLER DETERMINES THE PURPOSES AND MEANS OF THE PROCESSING OF PERSONAL DATA

- The Controller has the power to determine:
- -Why the processing will take place
- -For which purpose

CONTROL STEMMING FROM LEGAL PROVISIONS

(E. VAGENA, TRADATA 2, 2022)

- Article 4(7)states that "where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."
- When the law establishes a task or impose a duty on someone to collect and process certain data.
- Example: Legal provisions The national law in Country A lays down an obligation for municipal authorities to provide social welfare benefits such as monthly payments to citizens depending on their financial situation. In order to carry out these payments, the municipal authority must collect and process data about the applicants' financial circumstances. Even though the law does not explicitly state that the municipal authorities are controllers for this processing, this follows implicitly from the legal provisions.

CONTROL STEMMING FROM FACTUAL INFLUENCE

(E.VAGENA, TRADATA 2, 2022)

- The need for factual assessment means that the role of a controller does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. The same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity.
- Certain processing activities can be considered as naturally attached to the role or activities of an entity ultimately entailing responsibilities from a data protection point of view
- Example: Providing an electronic communications service such as an electronic mail service involves processing of personal data. The provider of such services will normally be considered a controller in respect of the processing of personal data that is necessary for the operation of the service as such (e.g., traffic and billing data). If the sole purpose and role of the provider is to enable the transmission of email messages, the provider will not be considered as the controller in respect of the personal data contained in the message itself. The controller in respect of any personal data contained inside the message will normally be considered to be the person from whom the message originates, rather than the service provider offering the transmission service.

"MEANS AND PURPOSES"

- To determine the means and purposes of the processing, the Controller must answer to the "why" and the "how" of the processing:
- why is the processing taking place?
- how will this objective be reached?
- It is sometimes legally challenging to set the level of influence on the "why" and the "how" that a Controller and a Processor has so that they can be set apart.

MEANS AND PURPOSES

(E. VAGENA, TRADATA 2, 2022)

- As regards the determination of means, a distinction can be made between essential and non-essential means.
- ''Essential means'' are traditionally and inherently reserved to the controller. While non-essential means can also be determined by the processor, essential means are to be determined by the controller.
- "Essential means" are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?").
- Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate.
- "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard-or software or the detailed security measures which may be left to the processor to decide on.

MEANS AND PURPOSES

(E. VAGENA, TRADATA 2, 2022)

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

DATA PROTECTION BY DESIGN AND BY DEFAULT (A. 25)

- "1.Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
- 2.The controller shall implement appropriate technical and organizational measures for ensuring that, **by default,** only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. [...]"

JOINT CONTROLLERS (A. 26)

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

JOINT CONTROLLERS (A. 26)

(E. VAGENA, TRADATA 2, 2022)

-the qualification of joint controllers will mainly have consequences in terms of allocation of obligations for compliance with data protection rules and in particular with respect to the rights of individuals.

-joint controllership exists with regard to a specific processing activity when different parties determine jointly the purpose and means of this processing activity

-Not all processing involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.

-Usually, joint participation will take the form of a common decision(=intention) taken by two or more entities or result from converging decisions by two or more entities regarding the purposes and essential means

-Decisions can be considered as converging on purposes and means if they complementeach other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing

JOINT CONTROLLERS (A. 26)

(E. VAGENA, TRADATA 2, 2022)

- Two or more entities have exerted influence over the means of the processing.
- Also covers the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity which decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.
- The use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context.
- The use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing)

JOINT CONTROLLERS EXAMPLE

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

PROCESSOR (A.28)

- "a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller"
- might be an organisation, but it might also be an individual
- Two basic conditions for qualifying as processor are: a)being a separate entity in relation to the controller and Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot be a processor to another department within the same entity. b)processing personal data on the controller's behalf. A processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means.
- As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.

OBLIGATIONS OF THE PROCESSOR

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

DUTY OF THE CONTROLLER

- The controller has the duty to use "only processors providing sufficient guarantees to implement appropriate technical and organizational measures",
- The controller is therefore responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration.
- The guarantees "provided" by the processor are those that the processor is able to demonstrate to the satisfaction of the controller, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations.
- The obligation to use only processors "providing sufficient guarantees" contained in Article 28(1) GDPR is a continuous obligation. It does not end at the moment where the controller and processor conclude a contract or other legal act. Rather the controller should, at appropriate intervals, verify the processor's guarantees, including through audits and inspections where appropriate

DATA PROCESSING AGREEMENT

- Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

CONTENT OF THE DPA

(E. VAGENA, TRADATA, 2022)

- the subject-matter of the processing (for instance, video surveillance recordings of people entering and leaving a high-security facility).
- the duration of the processing: the exact period of time, or the criteria used to determine it, should be specified;
- the nature of the processing: the type of operations performed as part of the processing (for instance: "filming", "recording", "archiving of images", ...) and purpose of the processing (for instance: detecting unlawful entry). This description should be as comprehensive as possible, depending on the specific processing activity, so as to allow external parties (e.g. supervisory authorities) to understand the content and the risks of the processing entrusted to the processor.
- the type of personal data: this should be specified in the most detailed manner as possible (for instance: video images of individuals as they enter and leave the facility). It would not be adequate merely to specify that it is "personal data pursuant to Article 4(1) GDPR" or "special categories of personal data pursuant to Article 9". In case of special categories of data, the contract or legal act should at least specify which types of data are concerned, for example, "information regarding health records", or "information as to whether the data subject is a member of a trade union";
- the categories of data subjects: this, too, should be indicated in a quite specific way (for instance: "visitors", "employees", delivery services etc.);
- the obligations and rights of the controller: the rights of the controller are further dealt with in the following slides (e.g. with respect to the right of the controller to perform inspections and audits).

PROCESSOR AND CONTROLLER

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

PROCESSOR AND CONTROLLER

- The Processor assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
- The Processor, at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- The Processor makes available to the controller all information necessary to demonstrate compliance with the above obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
- the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

PROCESSOR AND CONTROLLER

- Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to above shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

RECORDS OF PROCESSING ACTIVITIES (A. 30)

- 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:
- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;
- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- (e) where applicable, transfers of personal data to a third country or an international organisation,
- (f) where possible, the envisaged time limits for erasure of the different categories of data;
- (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

RECORDS OF PROCESSING ACTIVITIES (A. 30)

- Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- (b) the categories of processing carried out on behalf of each controller;
- (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

REPRESENTATIVES (A. 27)

- «1.Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.[**ar. 3 (2)
- 2.This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:(a)the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b)the monitoring of their behaviour as far as their behaviourtakes place within the Union.]2.The obligation laid down in paragraph 1 of this Article shall not apply to:(a)processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b)a public authority or body.

REPRESENTATIVES (A. 27)

- [...] 3.The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.
- 4.The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.5.The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.»

THANK YOU FOR YOUR ATTENTION!

- ILIANA KOSTI

- Iliana_Kosti@yahoo.gr

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

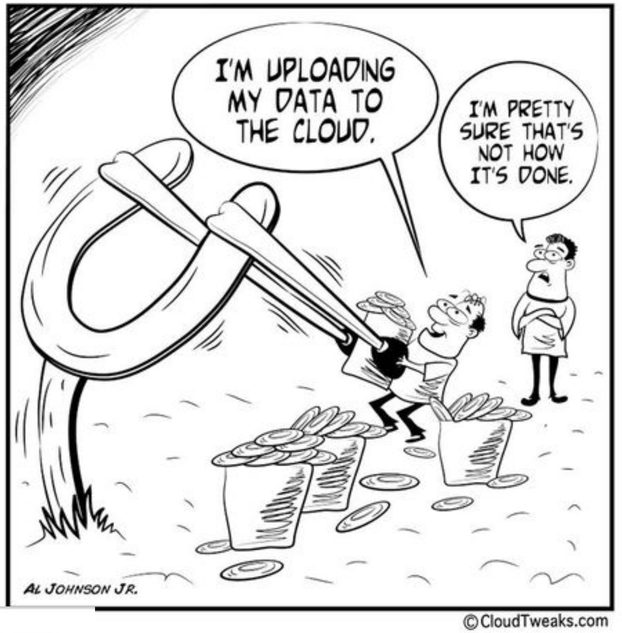
Transfers of personal data to third countries

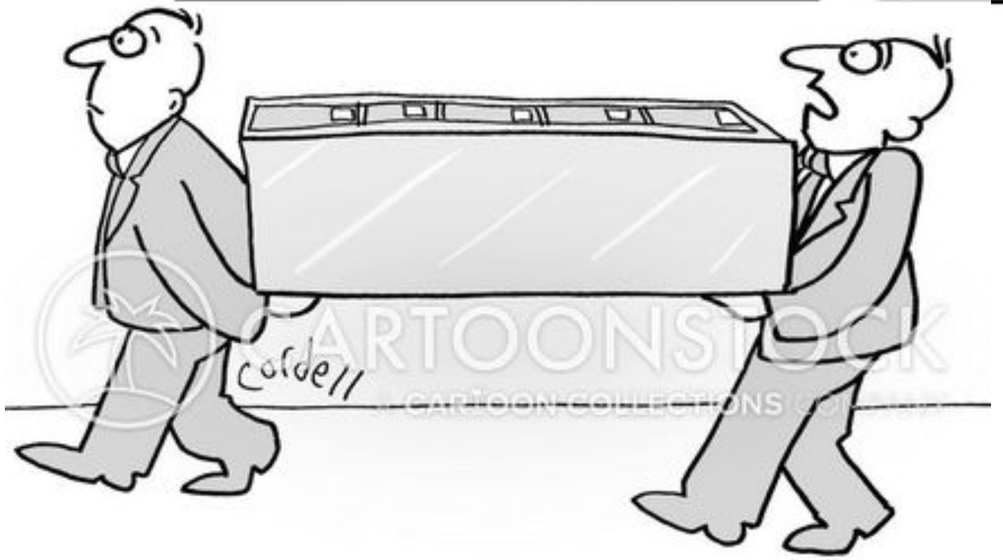
Nicola Fabiano

Athens, 23 June 2023

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

Transfers of personal data to third countries or international organisations





"Surely there's an easier way of moving files?"

Transfers of personal data to third countries or international organisations

CHAPTER V

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

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

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

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

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

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

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

Is that regulation in the GDPR only in Chapter V?
No, see also Articles: 3 - 15(1)(c) - 30(1)(d) - 40(3) - 96 - Convention 108/1981 - Article 14

EDPB Guidelines n. 5/2021

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

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

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

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

EDPB Guidelines 5/2021 - 1st crit.

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

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

EDPB Guidelines 5/2021 - 2nd crit.

The **second criterion** requires that there is a controller or processor disclosing by transmission or otherwise making data available to another controller or processor. These concepts have been further elaborated on in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. It should, inter alia, be kept in mind that the concepts of controller, joint controller and processor are functional concepts in that they aim to allocate responsibilities according to the actual roles of the parties and autonomous concepts in the sense that they should be interpreted mainly according to EU data protection law. A case-by-case analysis of the processing at stake and the roles of the actors involved is necessary.

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

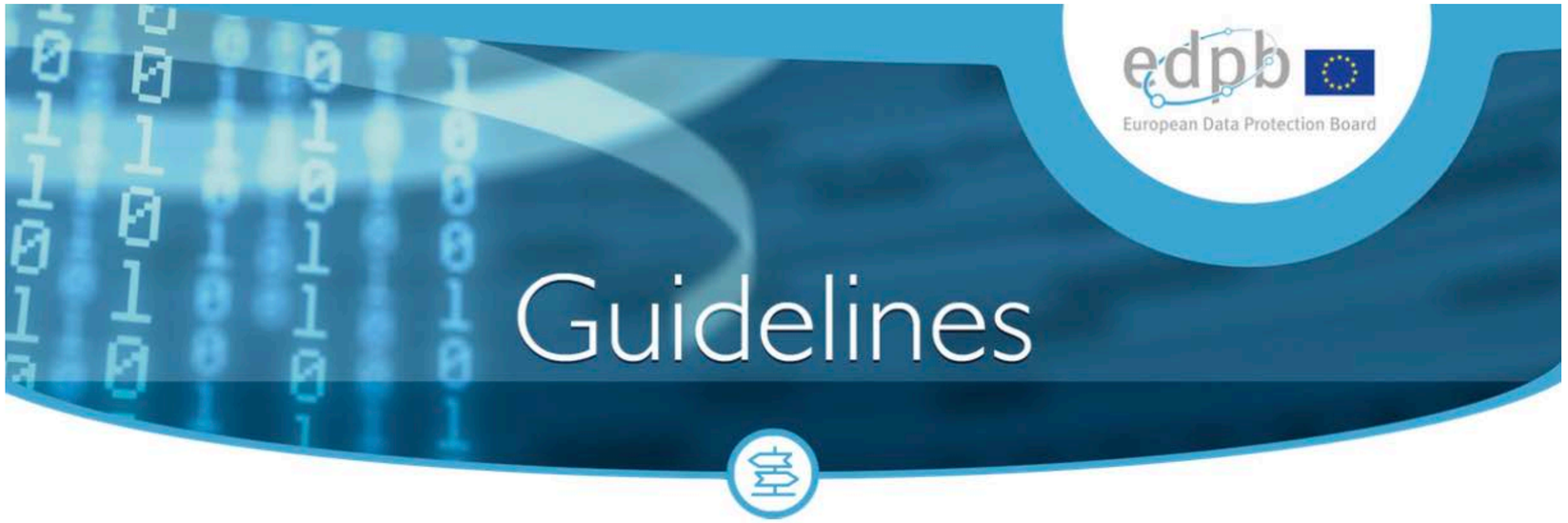
EDPB Guidelines 5/2021 - 3rd crit.

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

EDPB Guidelines 5/2021 - Conclusions

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

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

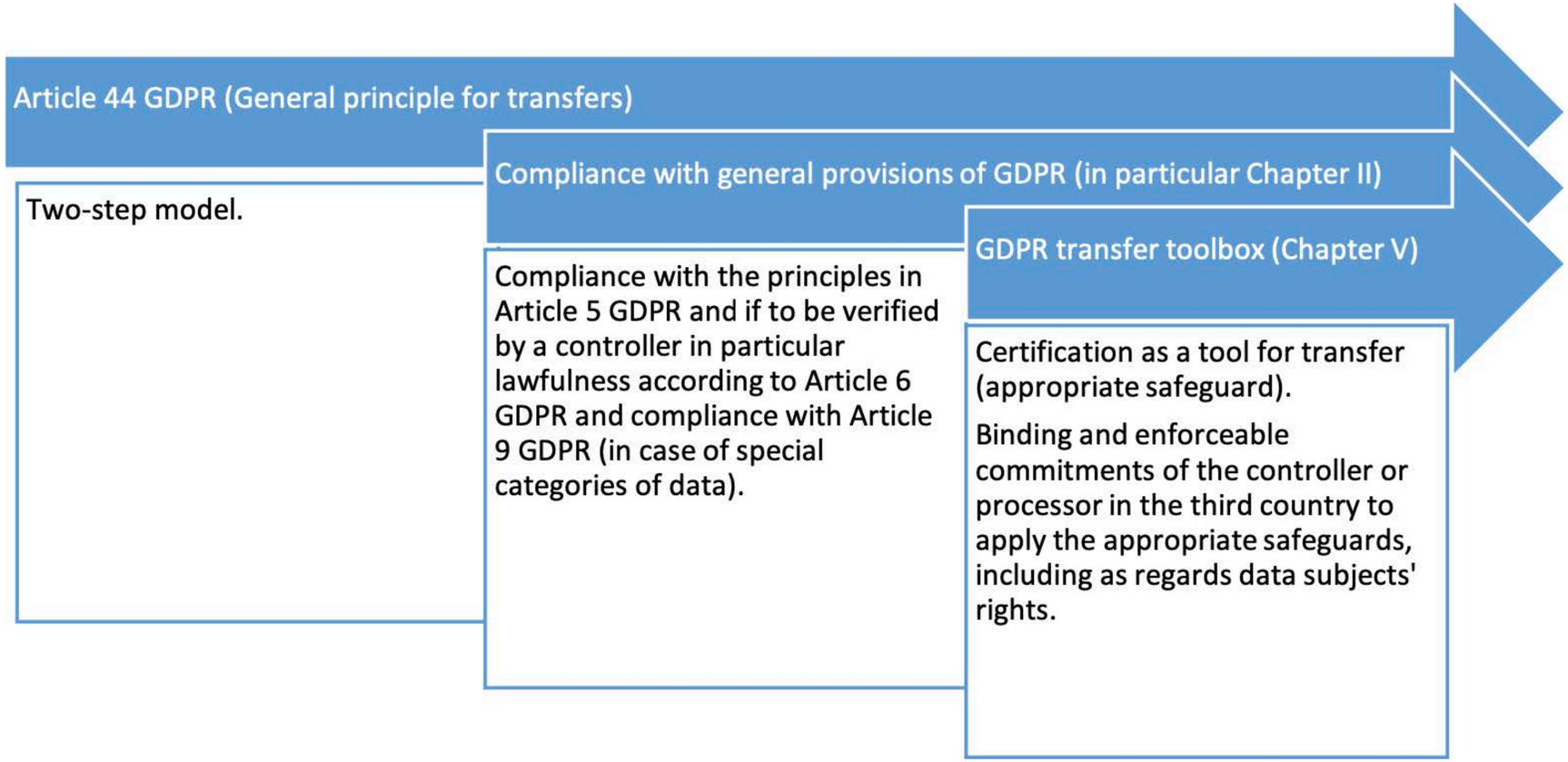


Guidelines 07/2022 on certification as a tool for transfers

Version 2.0

Adopted on 14 February 2023

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



1.2 General rules applicable to international transfers

4. *… Pursuant to Article 46 (2) (f) of the GDPR, such appropriate safeguards **may be provided for by an approved certification mechanism** together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.*

5. *As a result, **the data exporter might decide to rely on the certification obtained by a data importer as an element to demonstrate compliance with its obligations** e.g. according to Article 24 (3) or Article 28 (5) GDPR. **The data importer might decide to apply for certification to demonstrate that appropriate safeguards are in place**.*

General principles

General principles

Subjective scope

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

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

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

Article 6 § 4

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

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

Article 2 § 1

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

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

Article 3 § 4

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

General principles

Article 44
General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another internat ional organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

See also W(102)-W(102)

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

Conditions for transfer under the GDPR

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

The adequacy decision

Adequacy decisions

European Commission website

Adequacy of the protection of personal data in non-EU countries

Adequacy decisions - Article 45

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

Previous decisions Article 45(9)

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

See also:

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

STUDIO LEGALE FABIANO

Transfers EU-USA-EU

Transfers EU-USA - Safe Harbour

Once upon a time the "Safe Harbour"

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

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

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

Transfers EU-USA - Privacy Shield

Once upon a time the "Privacy Shield"

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

From the European Commission website

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

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

What was happening in 2018 ....

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

Document instituting the proceedings

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

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

Shrems II Judgement

Judgment of the Court (Grand Chamber) of 16 July 2020 in Case C-311/18 - REQUEST for a preliminary ruling under Article 267 TFEU from the Hi 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

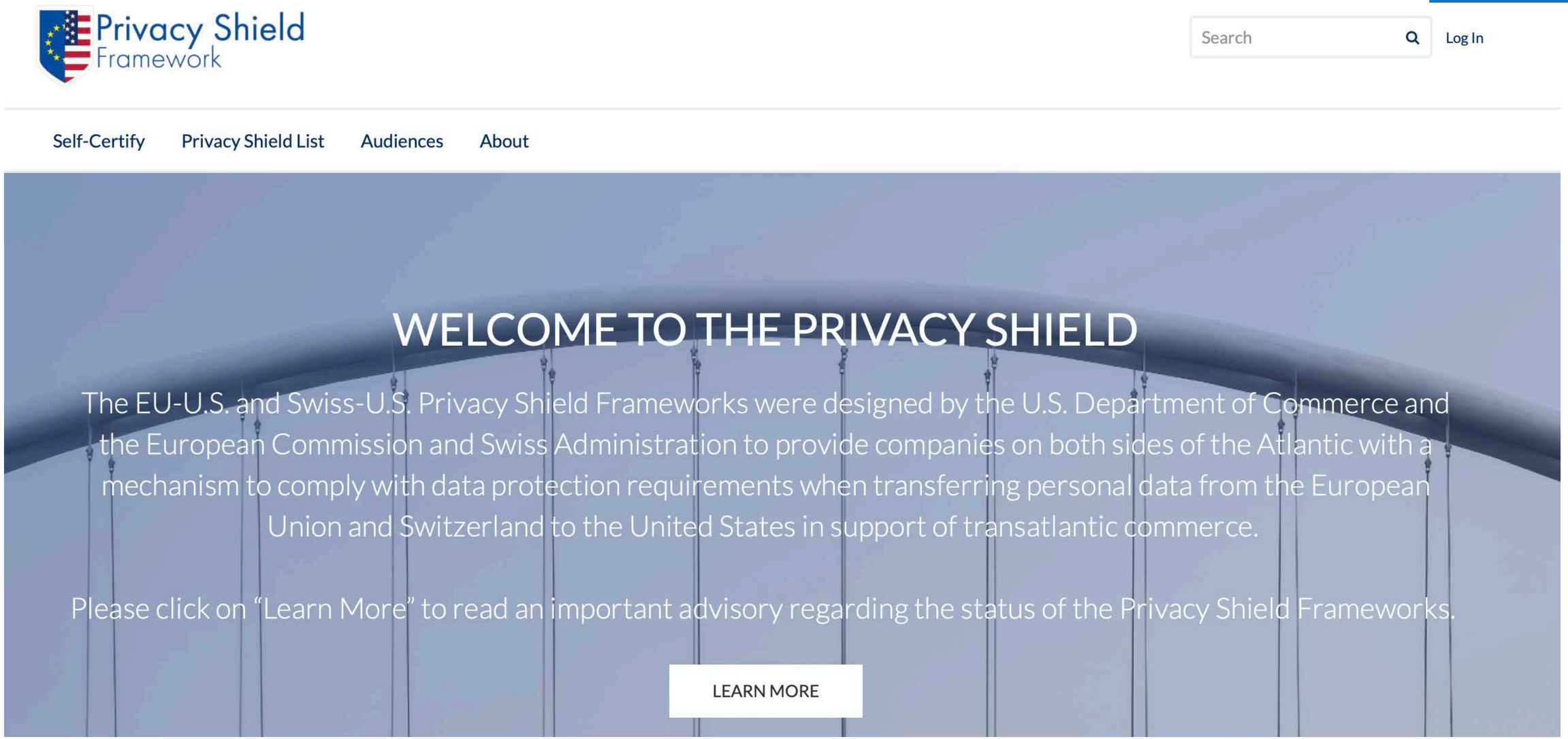
[European Data Protection Board publishes FAQ document on CJEU judgment C-311/18 (Schrems II)]

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



OCTOBER 07, 2022

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

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

Press release - 28/2/2023

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

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

Adopted on 28 February 2023

Transfers subject to appropriate safeguards

Transfers subject to appropriate safeguards

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

Previous authorizations Article 46(5)

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

* With the authorisation of the supervisory authority

See also:

- *W108*
- *W109*
- *W114*

Standard Contractual Clauses - SCC

Model clauses prior to the current ones

Nomenclature

Standard data protection clauses

Model Contractual Clauses

Model clauses

EU controller - non-EU or EEA controller

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

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

EU controller - non-EU or EEA processor

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

Standard Contractual Clauses (SCC)

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

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

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

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

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

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

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

SCC advantages

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

How some big "players" behave ...

Google

Google Privacy & Terms

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

- Introduction
- Information Google collects
- Why Google collects data
- Your privacy controls
- Sharing your information
- Keeping your information secure
- Exporting & deleting your information
- Retaining your information
- Compliance & cooperation with regulators
- About this policy
- Related privacy practices
- Data transfer frameworks
- Key terms
- Partners
- Updates

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

GOOGLE PRIVACY POLICY

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

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

Privacy Checkup

Looking to change your privacy settings?

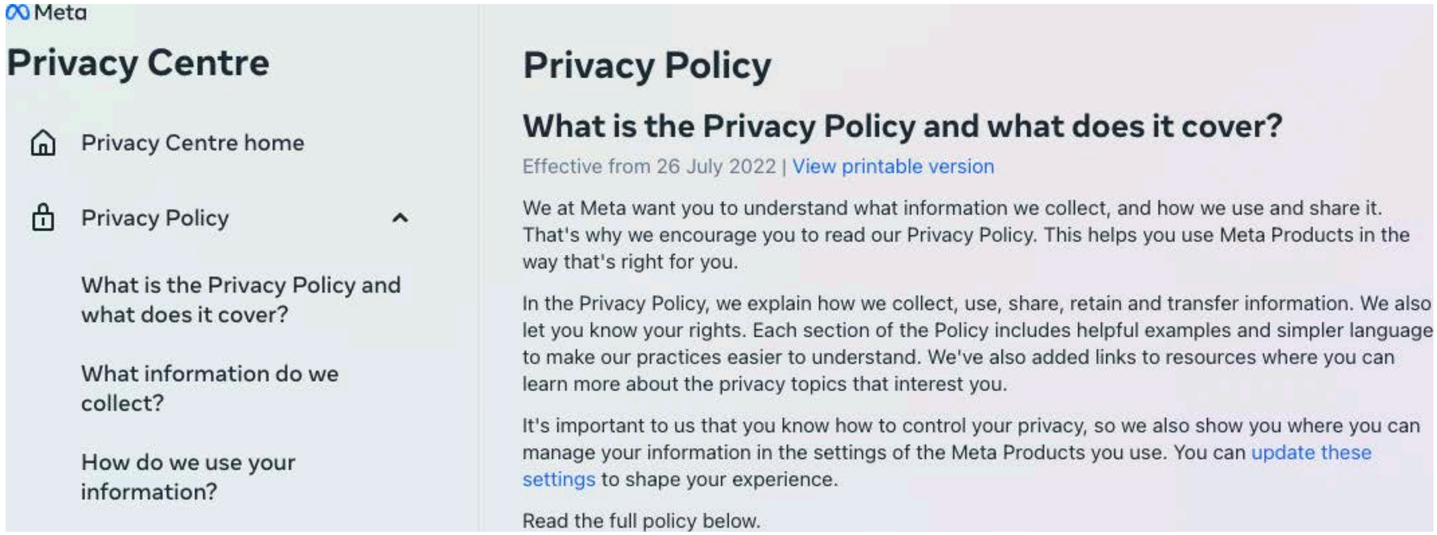
Take the Privacy Checkup

Effective February 10, 2022 | Archived versions | Download PDF

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

Facebook (Meta)
&
Privacy Shield

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



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

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

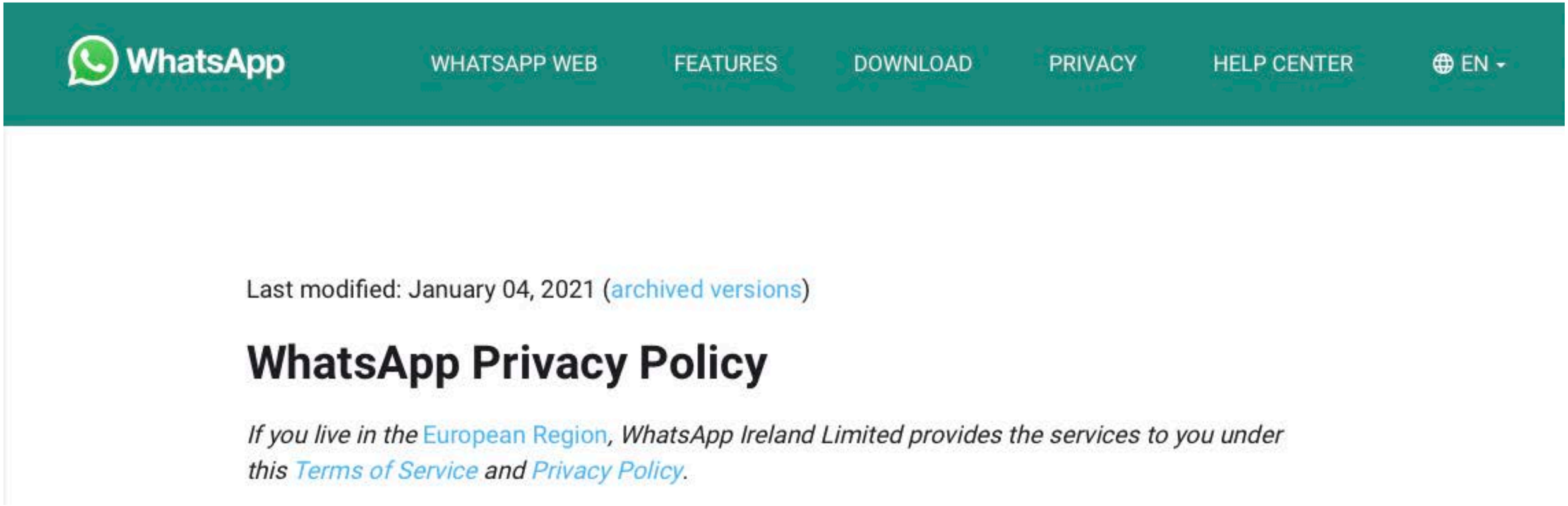
Meta Platforms, Inc. ("Meta") has certified to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, "Privacy Shield Frameworks") with the US Department of Commerce regarding the collection and processing of personal data from our advertisers, customers, or business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

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.

Whatsapp



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

Amazon

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.**

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.

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: privacyshield@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

Apple

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

Apple Privacy Policy

Updated October 27, 2021

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

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

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

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

Download a copy of this Privacy Policy (PDF)

Your California Privacy Disclosures ›
Information Regarding Commercial Electronic Messages in Canada ›
Apple Health Study Apps Privacy Policy ›

Transfer of Personal Data Between Countries

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

Binding Corporate Rules (BCR)

BCR - Definitions

Article 4(20)

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

Article 4(19)

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

BCR - Schema

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

See also:

- *W110*
- *W167-168*

Summary of the procedure for BCRs

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

Template for the BCR

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

WP265

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

Standard Application for Approval of Binding Corporate Rules for Processors

PART 1: APPLICANT INFORMATION

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

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

Does the Group have its headquarters in the EEA?

☐ Yes
☐ No

Name and location of the applicant:

Identification number (if any):
Legal nature of the applicant (corporation, partnership, etc.):

Description of position of the applicant within the Group:
(e.g. headquarters of the Group in the EEA, or, if the Group does not have its headquarters in the EEA, the member of the Group inside the EEA with delegated data protection responsibilities)

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

Address:

Country:
Phone number: Fax: E-Mail:

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

Approved BCR

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

A list of **pre-GDPR BCR approved** before 25 May 2018 -> on the EDPB website

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

Derogations for specific situations

Derogations for specific situations

Prerequisites - art. 49(1)

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

Conditions - art. 49(1)

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

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

See also: W111-114

Thank you for your attention!

Nicola Fabiano

https://bio.link/nicfab

@nicfab

LinkedIn

@nicfab@nicfab.it

Privacy Community

NicFab Channel

STUDIO LEGALE FABIANO

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

The EU Directive 2016/80, its implementation thus far and its incorporation into Greek law

Niki Giannakou

Athens, 23 June 2023

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

I. Introduction to the Directive (EU) 2016/80

LAWYERS

DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

"on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA"

Why do we need a separate legal framework from the GDPR for the processing of data by police and judicial authorities?

Point 3 of the explanatory memorandum: *"Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.*"

Recital 4 of the explanatory memorandum: "*The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.".*

LAWYERS

Legal regime prior to the adoption of the Directive:

→ ***Framework Decision 2008/977/JHA***

- processing of personal data by police and judicial authorities
- explicitly repealed by Article 59 of the Directive

Why was this legal framework established through the adoption of an EU Directive instead of an EU Regulation?

FA LAWYERS

→ The competent institutions took into account that each Member State has different legal traditions and functions at the level of police and judicial authorities

Point 11 of the explanatory memorandum: *"It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. […]".*

LAWYERS

II. The main provisions of Directive EE2016/80

LAWYERS

1st Chapter

Scope of application

- The activities of European organizations are not covered by the Directive.
- The Directive does not apply to the processing of personal data in the context of an activity which falls outside the scope of Union law.
- Activities relating to national security do not fall under the scope of Union law.
- Member States have legislative flexibility in the sensitive issue of national security.
- There is no clear distinction between public security and national security.

LAWYERS

Key definitions of the Directive – Article 3

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(6) ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

(7) **‘competent authority’** means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

The definition of 'competent authority' encompasses:

- Police
- Judicial authorities
- Other public authorities that undertake preliminary investigations

2nd Chapter

General principles of data processing

- ***(Art. 4)*** The fundamental principles of data minimization, purpose limitation, lawfulness, transparency, accuracy, integrity and confidentiality of the GDPR are reiterated in Art. 4 of the Directive.
- ***(Art. 5)*** Establishment of appropriate time limits for data erasure and storage.
- ***(Art.6)*** Distinction between different categories of data subject.
- ***(Art. 7)*** Distinction between personal data and verification of quality of personal data.
- ***(Art. 8)*** Lawfulness of processing.
- ***(Art. 9)*** Establishment of specific processing conditions.
- ***(Art. 10)*** Processing of special categories of personal data.

LAWYERS

Automated individual decision-making

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

3rd Chapter
Rights of the data subject

- ***(Art. 12)*** Communication and modalities for exercising the rights of the data subject

→ *The Directive provides that Member States should facilitate the exercise of rights by citizens without imposing bureaucratic difficulties and financial costs on them, by providing them with information in simple and comprehensible language so that they can effectively exercise the rights provided for.*

- ***(Art. 13)*** Information to be made available or given to the data subject

→ *It provides, inter alia, that information should be given on the identity and contact details of the controller, the contact details of the data protection officer, where applicable, the purposes of the processing for which the personal data are intended, the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority.*

LAWYERS

- ***(Art. 14)*** Right of access by the data subject
- ***(Art. 15)*** Limitations to the right of access
- ***(Art. 16)*** Right to rectification or erasure of personal data and restriction of processing
- ***(Art. 17)*** Exercise of rights by the data subject and verification by the supervisory authority

→ Article 17 provides that in cases where the rights of information, access, rectification or erasure of personal data of the data subjects are limited or not met, the data subject may apply to the Supervisory Authority, provided for in Article 41. This arrangement introduces an additional safeguard to ensure that competent authorities do not act arbitrarily when processing data subjects' data and are subject to the necessary control.

- ***(Art. 18)*** Rights of the data subject in criminal investigations and proceedings

LAWYERS

Remaining Chapters

Obligations of data controllers and data processors

- Data controllers under the Directive must implement appropriate technical and organizational measures, taking into account the nature and purpose of the processing they carry out and the risks to the rights and freedoms of data subjects arising from such processing.

- Competent authorities are obliged to apply the principles of data protection by design and by default.

- Triple supervision mechanism in the process of processing of personal data by the competent authorities:
  - DPO
  - Independent Supervisory Authorities
  - European Data Protection Board

LAWYERS

III. Incorporation of the Directive in the national laws of Member States

- The incorporation of the Directive into the national laws of the Member States is significantly delayed.

- The Commission is also required to ensure that the Directive has been adequately transposed.

- In its first report on the implementation and functioning of the Data Protection Directive in the context of law enforcement (EU) 2016/680 dated July 2022, the Commission found the implementation of the Directive satisfactory.

- Thus far the Commission has taken legal action against Spain, Germany and Greece.

IV. Jurisprudence of the ECJ

1. *WS v Bundesrepublik Deutschland, C-505/19, EU:C:2021:376*

The Court did not rule out the lawfulness of the processing of personal data contained in a red alert issued by Interpol until it is established, by a final judicial decision, that the *ne bis in idem* principle applies to the acts on which that alert is based. The Court concluded with this judgment, reasoning *inter alia* that *"In particular, on the one hand, the transmission of the data in question by Interpol does not constitute processing of personal data falling within the scope of Directive 2016/680, since that body is not a 'competent authority' within the meaning of Article 3(7) of that directive"*, while on another point it held that *"It must, however, be recalled that, where it has been established, by means of a final judgment delivered in a Contracting State or in a Member State, that a red notice issued by Interpol in fact relates to the same acts as those for which the person concerned by that notice has already been finally judged and that, consequently, the principle of ne bis in idem applies, that person (. .) can no longer be prosecuted for the same acts and, consequently, can no longer be arrested in the Member States for those acts."*.

LAWYERS

2. B v Latvijas Republikas Saeima, C-439/19, EU:C:2021:504

The Court interpreted "competent authority" by excluding the Latvian Road Safety Directorate from the concept of competent authority under Article 3(7) of the Directive. Furthermore, in that judgment the Court set out the following criteria for the classification of an infringement as a criminal offence: (1) whether the infringement is classified as a criminal offence under national law; (2) the nature of the infringement itself; and (3) the degree of severity of the sanction which is threatened against the person concerned.

3. ECJ C-205/21

The Court of Justice has, *inter alia*, interpreted Article 10 of the Directive by providing, that the processing of biometric and genetic data by police authorities in the course of their investigative activities for the purposes of combating crime and maintaining public order is permitted under the law of a Member State within the meaning of Article 10(a) of the Directive where the law of the Member State provides for a sufficiently clear and precise legal basis for the processing of biometric and genetic data.
Furthermore, the Court of Justice has interpreted Article 6 in that regard, stating that said provision does not preclude national legislation which provides that, where a person accused of intentionally committing an offence which is prosecuted ex officio refuses to cooperate voluntarily in the collection of biometric and genetic data relating to him or her for the purpose of recording them, the competent criminal court is obliged to order the compulsory collection of that data, without having the power to assess whether there are serious grounds for considering that the data subject has committed the offence of which he is accused, provided that national law subsequently ensures effective judicial control of the conditions on which the accusation on the basis of which the authorization to collect the data was granted was based.

However, the Court of Justice, making a combined assessment of Articles 10, 4(1)(a)-(c) and 8(1) and 2 of the Directive, held that those rules preclude national legislation which provides for the systematic collection of biometric and genetic data from any person accused of intentionally committing an offence against the law for the purpose of recording them, without providing that the competent authority must establish and demonstrate, first, that such collection is strictly necessary for the fulfilment of the specific purposes pursued and, second, that it is not possible to achieve those purposes by means of a moderate collection of biometric and genetic data.

V. The incorporation of the Directive in Greece

LAWYERS

Greece has not managed to transpose the Directive into its national law in time. The transposition of the Directive was done in 2019 in a single law with the provisions for the transposition of the GDPR into national law, Law 4624/2019. The national law incorporated the Directive for the most part but unfortunately did not fully comply with its provisions. This was also noted by the Commission, which in April 2022 initiated an infringement procedure against our country on the grounds that the national transposition legislation in question does not comply with the Directive.

In December 2022, Greece has largely amended the relevant national law to meet the Commission's criteria, thus offering greater security to data subjects. So far there is no feedback from the Commission's expert team

Concluding Remarks

Thank you very much!

FA LAWYERS

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

Principles of data processing

Spyridon Tassis

Athens, 23 June 2023

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

The GDPR

- The General Data Protection Regulation (GDPR) is a regulation that addresses the protection of personal data and the privacy rights of individuals. While the GDPR does not explicitly define "processing principles," it establishes several key principles that govern the processing of personal data.

- Over the past three decades, data access, sharing and use have become central drivers of economic growth and social well-being. Data, and in particular their processing and sharing, have become an integral part of every sector of the economy as well as a critical source of innovation for disruptive technologies such as the Internet of Things and Artificial Intelligence.

- However, the ubiquitous exchange of data across entities has amplified a range of concerns for governments, businesses, and citizens, eroding trust among them.

- In response to this erosion of trust, policies and regulations have set principles for the personal data processing and flows motivating controllers and processors to be aware of their processing activities and data subjects to be aware of their rights.

What is the real issue here?

- Vast computing power combined with huge databases around the world
- Multinational companies that need to process and circulate data
- Numerous online services (cloud-based services) creating cyber-anxiety
- Data analytics (especially Google) that create added value information
- Data rights that need to be respected
- Lack of data subject control of its data
- So how we ensure compliance?
- Digital Humanism

Which activities are affected?

- Oh, all that data (the new fuel, the new money, the new economy etc.)
- AdTEch, IoT, Big Data, Analytics, cloud services are the new competition fields
- A market demand that drives (forces?) the regulatory necessity
- It’s a data driven economy so data processing is everywhere
- The size of the controller/processor is irrelevant
- ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Why are processing principles essential?

Data processing principles are essential for several reasons:

- **Accuracy**: Data processing principles ensure that data is processed accurately, minimizing errors and inconsistencies.
- **Efficiency**: Following data processing principles helps optimize the efficiency of data processing operations.
- **Consistency**: Data processing principles promote consistency in handling and manipulating data.
- Privacy and Security: Data processing principles play a significant role in protecting the privacy and security of data.
- **Compliance**: Many industries and jurisdictions have specific regulations and compliance requirements regarding data processing.
- **Data Quality**: Effective data processing principles contribute to improving data quality.

Why are processing principles essential?

- **Scalability**: Data processing principles facilitate scalability and adaptability to changing business needs.
- **Decision-Making**: Reliable data processing principles provide a solid foundation for data analysis and decision-making.

Data processing principles are crucial for ensuring accuracy, efficiency, consistency, privacy, security, compliance, data quality, scalability, and reliable decision-making. By following these principles, organizations can effectively manage and utilize their data assets to drive business success.

Which are the GDPR data processing principles?

Chapter II – Article 5:

- **Lawfulness, Fairness, and Transparency.**
- **Purpose Limitation.**
- **Data Minimization.**
- **Accuracy.**
- **Storage Limitation.**
- **Integrity and Confidentiality.**
- **Accountability.**

Lawfulness, Fairness, and Transparency

The Lawfulness, Fairness, and Transparency principles, as outlined in the GDPR, set the groundwork for ethical and accountable processing of personal data. Let's delve deeper into each of these principles:

- **Lawfulness – 6.1: Processing personal data must have a valid legal basis as defined in the GDPR. The regulation provides several lawful bases for processing, including:**

  a. Consent
  b. Contractual Necessity
  c. Legal Obligation
  d. Vital Interests
  e. Public Task
  f. Legitimate Interests

Lawfulness, Fairness, and Transparency

- **Fairness:**

  a. Personal data must be processed in a fair manner.

  b. This means that individuals should be treated transparently and not subjected to any unjust or unexpected consequences as a result of the processing.

  c. Organizations must ensure that individuals are aware of how their data will be processed, the purposes for processing, and any potential impact on them.

  d. Fairness also entails avoiding unfair or discriminatory processing practices that might lead to unequal treatment or harm to individuals based on their personal characteristics or attributes.

Lawfulness, Fairness, and Transparency

- **Transparency – Article 12-14: Organizations are required to provide individuals with clear and concise information about the processing of their personal data. This includes:**

  a. Identity of the data controller
  b. Purposes of processing
  c. Legal basis
  d. Data retention period
  e. Recipients of the data
  f. Rights of individuals
  g. Data transfers

By adhering to the Lawfulness, Fairness, and Transparency principles, organizations ensure that individuals' rights and interests are respected, and they can make informed decisions about the processing of their personal data. Transparency promotes trust between individuals and organizations, fostering a more ethical and responsible data processing environment.

Purpose Limitation

The Purpose Limitation principle, as defined in the GDPR, emphasizes that personal data should be collected for specified, explicit, and legitimate purposes:

- **Specified Purposes**
- **Explicit Purposes**
- **Legitimate Purposes**
- **Compatibility between purposes**
- **Minimization of Data Collection**
- **Consent Alignment**

The Purpose Limitation principle aims to prevent the indiscriminate or unforeseen use of personal data. By requiring organizations to clearly define and communicate the purposes for data processing, it enhances transparency and empowers individuals to understand and control how their data is used. Organizations are encouraged to regularly review the purposes for which they process personal data and ensure ongoing compliance with the principle of Purpose Limitation.

TASSIS & ASSOCIATES LAW OFFICE

part of ICTLC group

Purpose Limitation – Exceptions

Where the processing for a purpose **other than that** for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Data Minimization

The **Data Minimization** principle, as outlined in the GDPR, emphasizes that organizations should collect and process only the personal data that is necessary for the specific purposes they have defined. Here are the key aspects of the Data Minimization principle:

- Limited Data Collection
- Purpose-Driven Data Collection
- Data Types
- Data Retention
- Data Minimization Techniques
- Privacy by Design and Default

The Data Minimization principle aims to enhance privacy and data protection by reducing the amount of personal data collected, processed, and stored. By adopting a data minimization approach, organizations can reduce the potential risks associated with data breaches, unauthorized access, and misuse of personal information. It also promotes transparency and accountability by ensuring that individuals have more control over their personal data and organizations are responsible stewards of that data.

Accuracy

The **Accuracy Principle**, as outlined in the GDPR, highlights the importance of ensuring the accuracy and currency of personal data. Here are the key aspects of the Accuracy principle:

- Data Quality
- Data Verification
- Timeliness
- User Participation
- Record-Keeping
- Communication with Third Parties
- Data Profiling and Decision-Making
- Data Subject Rights

By adhering to the Accuracy principle, organizations enhance the reliability and integrity of personal data. Accurate data is crucial for informed decision-making, maintaining trust with individuals, and complying with other data protection principles. Regular data validation, verification processes, and active involvement of individuals contribute to maintaining data accuracy over time.

Storage Limitation

The **Storage Limitation** principle (Data Retention), as defined in the GDPR, emphasizes that personal data should be stored for no longer than necessary for the purposes for which it was collected. Here are the key aspects of the Storage Limitation principle:

- Defined Retention Periods
- Purpose-Driven Storage
- Data Minimization
- Review and Disposal
- Legal Obligations and Business Needs
- Exceptions and Archiving
- Data Subject Rights

The Storage Limitation principle aims to promote responsible data management and minimize the risks associated with storing personal data for extended periods. By implementing proper retention practices, organizations can reduce the likelihood of unauthorized access, data breaches, or misuse of personal information. It also helps organizations maintain data accuracy and relevance, promoting compliance with other data protection principles such as Purpose Limitation and Data Minimization.

Integrity and Confidentiality

The **Integrity and Confidentiality** principle, as outlined in the GDPR, emphasizes the importance of protecting personal data against unauthorized access, alteration, disclosure, or destruction. Here are the key aspects of the Integrity and Confidentiality principle:

- Data Security Measures
- Confidentiality
- Data Protection by Design and Default
- Data Breach Notification
- Access Controls and Authentication
- Data Integrity
- Employee Training and Awareness

By adhering to the Integrity and Confidentiality principle, organizations can protect personal data from unauthorized access, maintain its accuracy and completeness, and prevent data breaches. Implementing robust security measures and promoting a culture of data protection contribute to maintaining individuals' trust, ensuring compliance with legal obligations, and safeguarding the rights and freedoms of data subjects.

Accountability

The **Accountability** principle, as outlined in the GDPR, emphasizes that organizations are responsible for complying with data protection laws and must demonstrate their compliance. Here are the key aspects of the Accountability principle:

- Proactive Compliance (Article 24)
- Data Protection Policies and Procedures (Article 24.2)
- Data Protection Impact Assessments (DPIAs – Article 35)
- Data Protection Officers (DPOs – Article 37))
- Records of Processing Activities (RoPA – Article 30)
- Data Breach Notification (Article 33)
- Cooperation with Supervisory Authorities (Article 39)
- Data Subject Rights (Chapter III - Articles 15-23)
- Vendor and Third-Party Management (Article 28)

The Accountability principle places the onus on organizations to actively demonstrate their compliance with data protection laws and regulations. By adopting a proactive and responsible approach to data protection, organizations can build trust with individuals, regulatory authorities, and other stakeholders. Accountability helps promote a culture of privacy and data protection within organizations and strengthens the overall data protection ecosystem.

Other data processing principles?

We should consider as data processing principles also the following obligations:

- **Data Subject Rights: The GDPR grants individuals certain rights regarding their personal data, such as the right to access, rectify, erase, restrict processing, and data portability. Organizations must facilitate the exercise of these rights and respond to data subject requests in a timely manner.**

- **Data Transfers: When transferring personal data outside the EU, organizations must ensure that adequate safeguards are in place to protect the data. This may involve using approved mechanisms like Standard Contractual Clauses or relying on recognized data protection frameworks.**

Landmark CJEU cases on principles of data processing

- **Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014)**
- **Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources (2014)**
- **Schrems v. Data Protection Commissioner (2015 and 2020)**
- **Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV (2019)**

Landmark CJEU cases on principles of data processing

- **Norra Stockholm Bygg AB v Per Nycander AB (2023)**
- **C-579/21 – Pankki S (2023)**

How the DPO or the Privacy advisor is implemented?

- should advise a controller or/and a processor on possible transfer issues
- should be implemented in the DPIAs and be aware of the processing activities and procedures, any data transfers (especially to third countries) and observe how the data subject rights are respected.
- If no adequate level of protection exists should advise for no data processing or transfer
- should pay special attention when reviewing art 28 (Data Protection Agreements) so all transfer issues are addressed in an accountable and clear manner.

Thank you

TASSIS & ASSOCIATES
LAW OFFICE

info@tassis.com

part of
ICTLC
group

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

The principle of consent: from theory to practice

Vassilis Karkatzounis

Athens, 23 June 2023

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

What is consent?

One of the six (6) available legal bases for personal data processing:

(a) Consent

(b) Performance of a contract

(c) Compliance with a legal obligation

(d) Vital interests

(e) Public interest / exercise of official authority

(f) Legitimate interests

What is consent?

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,

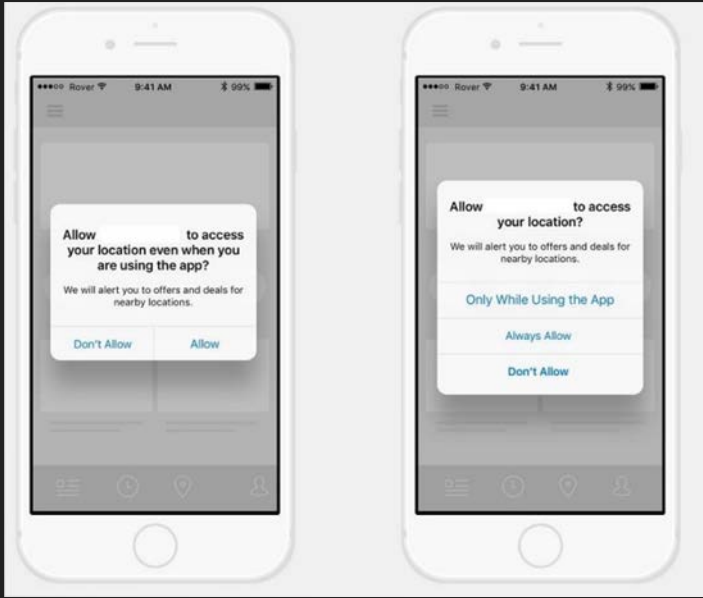
signifies agreement to the processing of personal data relating to him or her;

Article 4 par. 11 GDPR

Freely given

- ✓ Real choice and control → informational self - determination
- ✓ Imbalance of power as a factor for the assessment
- ✓ Conditionality and bundling
- ✓ Granularity and purpose limitation
- ✓ The issue of detrimental effects

Example 1



Example 2

Example 3

Cookies improve user experience

When you click 'Accept all' cookies, Aarhus University can give you the best user experience. Cookies store information about how a user interacts with a website. All your data is anonymised and cannot be used to identify you. You can always change your consent again under 'Cookies' in the website footer.

The university uses its own cookies and cookies set by our partners for the following purposes:

- [x] **STRICTLY NECESSARY**
  These cookies make it possible to use basic website functionality, e.g. navigation etc. The website does not work without these cookies.
- [ ] **STATISTIC**
  These cookies provide the university with anonymised data on how the user interacts with the website. For example, information about how often the user visits the website, and which pages the user visits.
- [ ] **TARGETING**
  These cookies make it possible for the university to target advertising on our websites and social media, so you will see the content that is most relevant for you.
- [ ] **FUNCTIONALITY**
  These cookies store information about the user's choices on the website such as language or login.

Accept selected | Accept all

Example 4

Specific

- ✓ Specific, explicit and legitimate purpose
- ✓ Granularity in consent requests
- ✓ Specific information
  - The reasonable expectations of data subjects
  - Big data … big problems ?

Example 5

Cable TV network collects subscribers' personal data, based on their consent, to present them with personal suggestions for new movies .

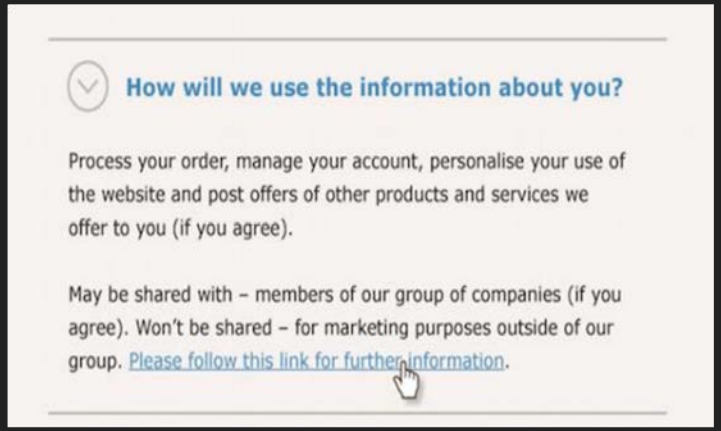
Cable TV network decides it would like to enable third parties to display targeted advertising on the basis of the subscriber's viewing habits.

Informed

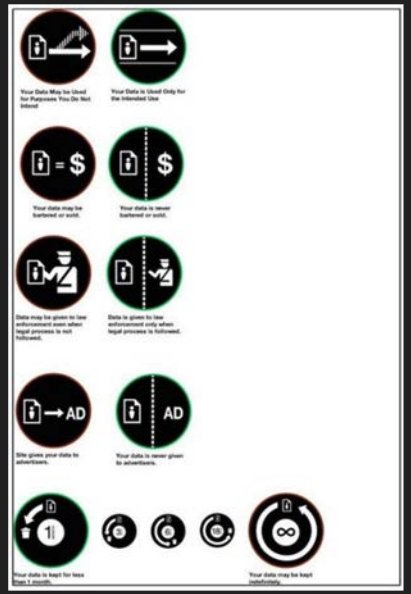
- ✓ Intelligible and easily accessible form, using clear and plain language
- ✓ Minimum content requirements
  - Who? the controller's identity
  - Why? the purpose of processing operations
  - What? the type of data collected and used
- ✓ How to provide information

Best practices

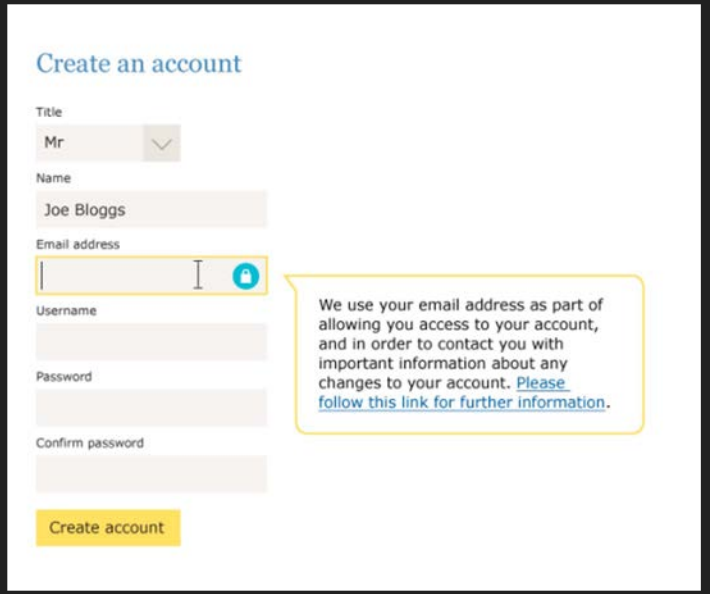
Layered Privacy Notice



Use of icons



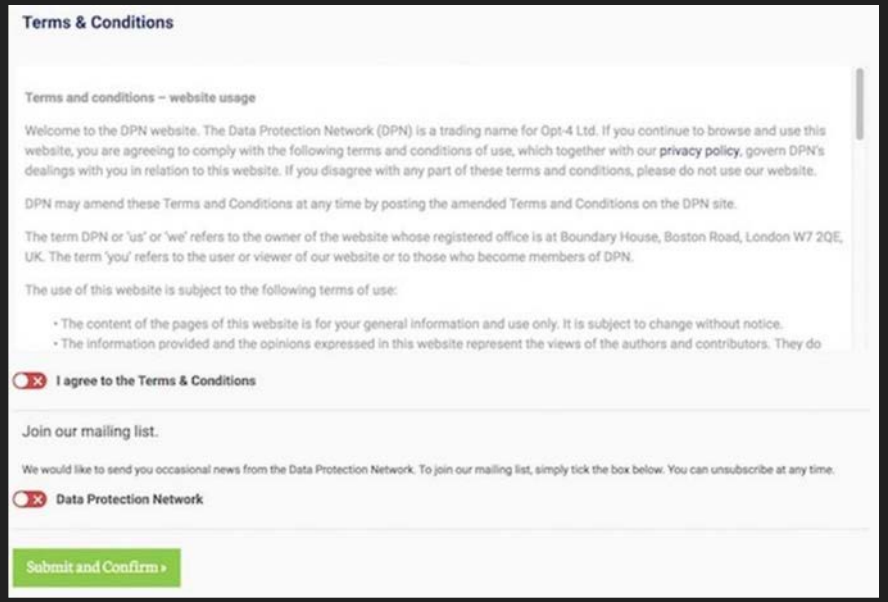
Just in time notice



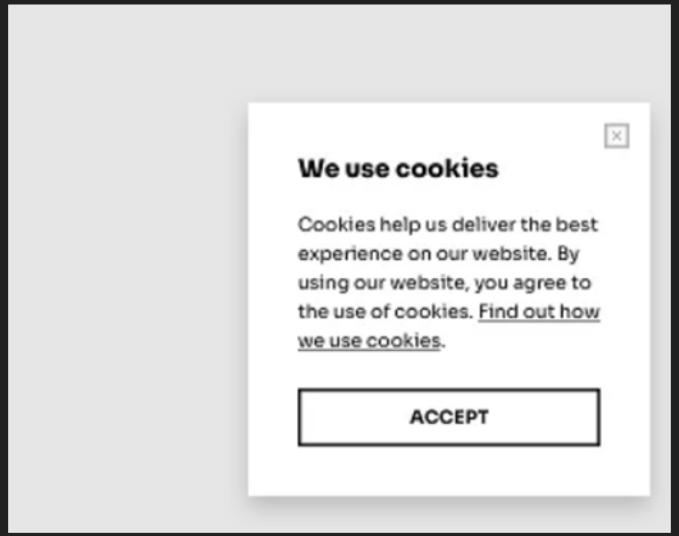
Unambiguous indication of wishes

- ✓ Statement or by clear affirmative action
- ✓ Written / oral / electronic form
- ✓ Not deriving from silence, inactivity or pre-ticked boxes
- ✓ No blanket acceptance of general terms and conditions (case of Meta)
- ✓ Consent flows and user experience

Example 6



Example 7



What about ‘explicit’ consent?

- ✓ Article 9 - processing of special categories of data
- ✓ Article 49 - data transfers to third countries
- ✓ Article 22 - automated individual decision-making
- ✓ Explicit = signed or recorded statement?
- ✓ 2-step verification of consent

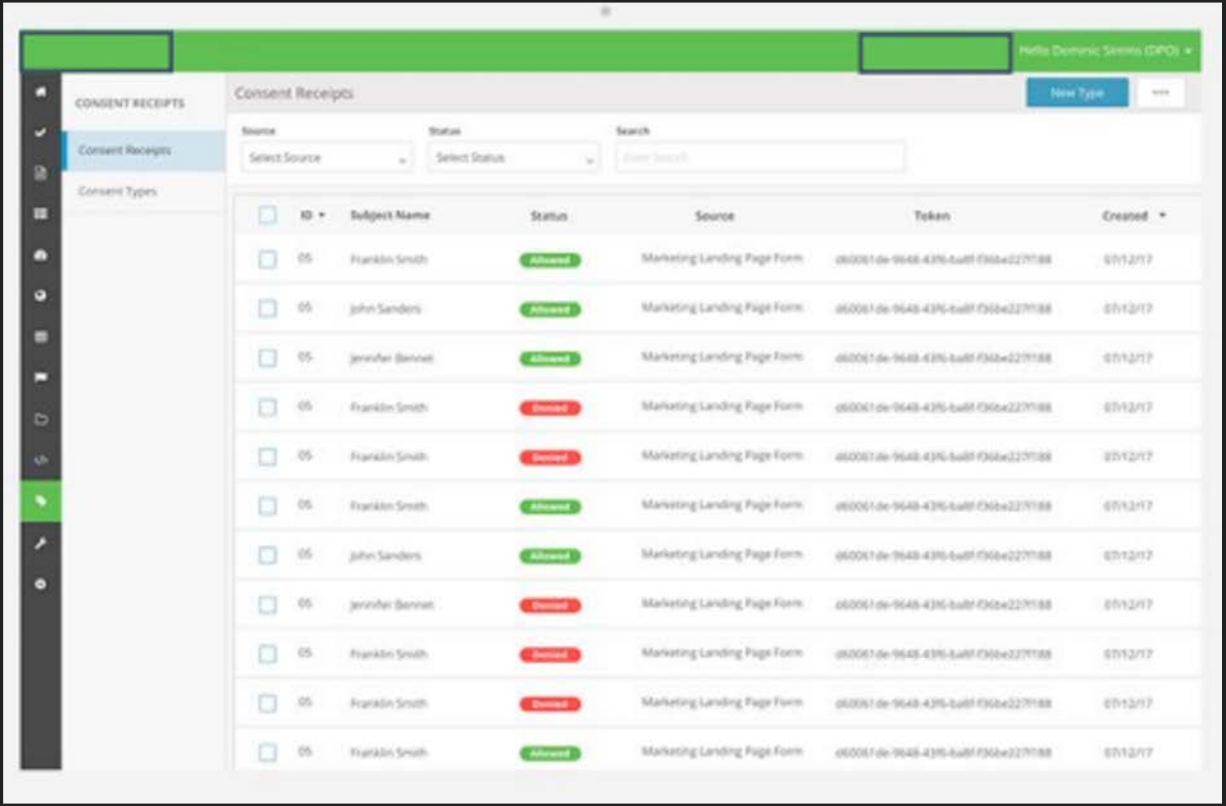
Example 8

Example 9

Demonstrating consent

- ✓ The burden of proof will be on the controller
- ✓ Show consent was obtained BUT don’t collect not necessary info
- ✓ A record of consent statements?
  - Who (is the data subject)
  - When (did he/she provide consent)
  - What (did he/she consent to)

Example 10


CONSENT RECEIPTS
Consent Receipts
Consent Types
Consent Receipts
New Type
Source
Select Source
Status
Select Status
Search
ID
Subject Name
Status
Source
Token
Created
Franklin Smith
John Sanders
Jennifer Bennet
Allowed
Denied
Marketing Landing Page Form

Special cases of consent

- ✓ Children in relation to information society services
  - information society services (as interpreted by the ECJ)
  - the age barrier
  - parental responsibility
- ✓ Scientific research
- ✓ ePrivacy consent

Some (constructive) criticism of consent

The rigidity and flatness of consent…

Should consent be enhanced or reshaped..?

Murky consent embraces the fact that consent in privacy is largely a set of fictions and is at best highly dubious.

Thank you for your attention!

Vassilis Karkatzounis,
Attorney at Law, CIPP/E, LL.M, PhD (c.)