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

Rights of the data subjects, including
rights in the context of automated decisions

Silvia Axinescu

Bucharest, 5 May 2023

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

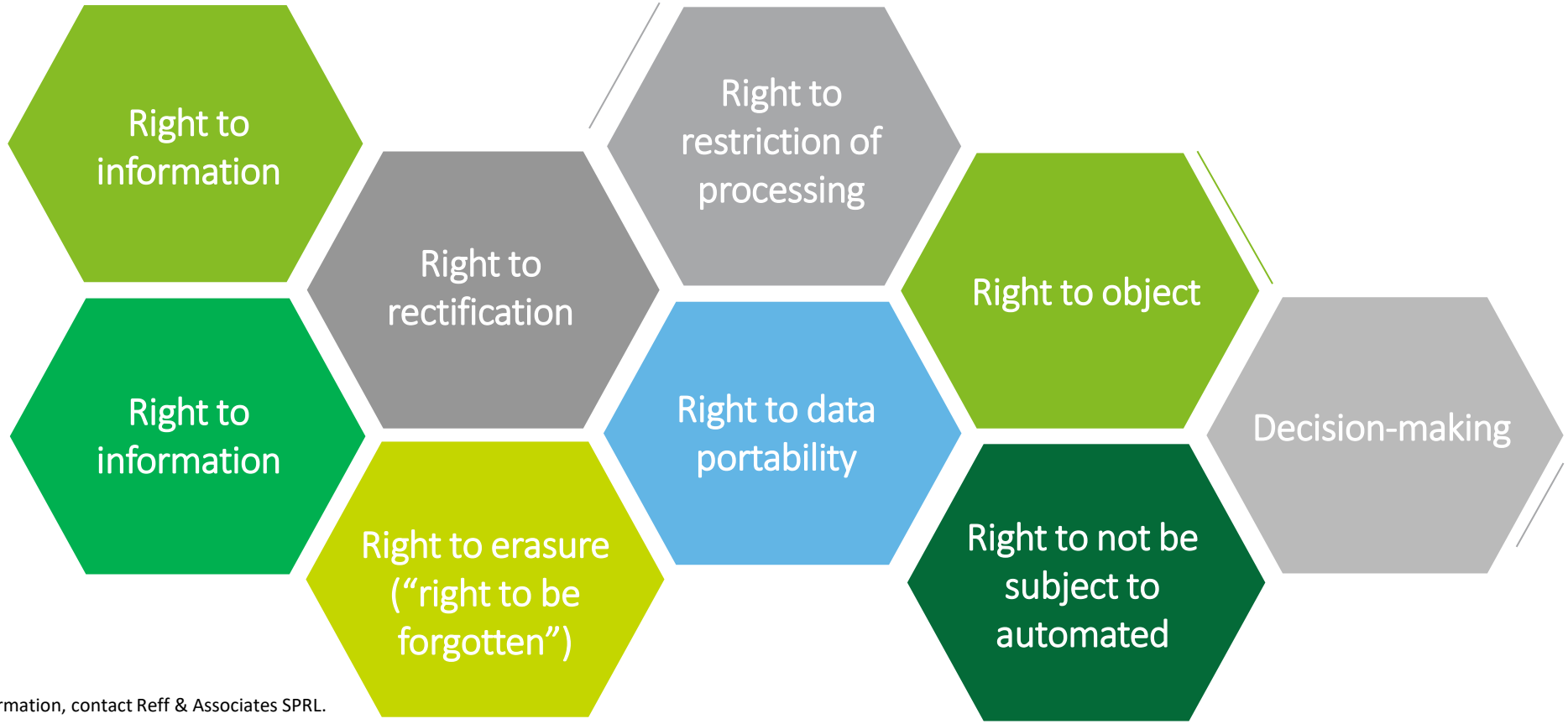
Rights of the data subjects, including rights in the context of automated decisions

Silvia Axinescu, lawyer Romanian Bar National Association

Training of Lawyers on EU Law relating to Data Protection 2

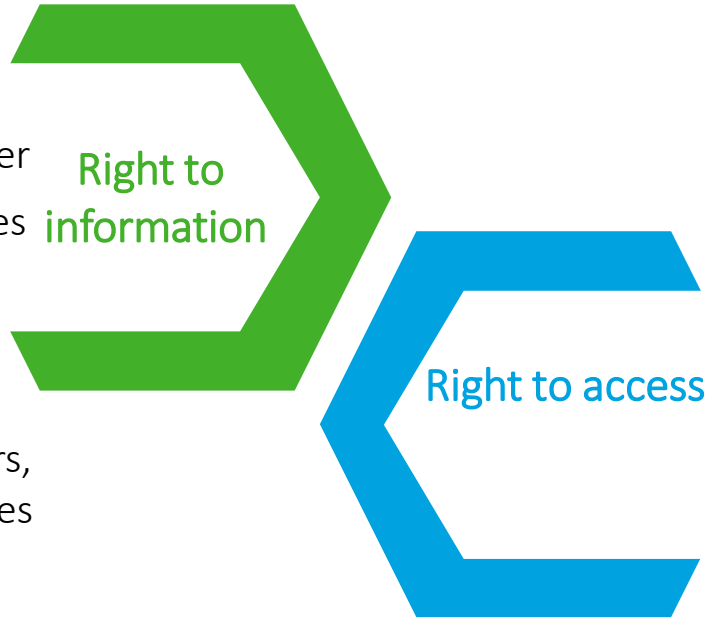
#TRADATA2

Which are the rights of the data subjects?



Key aspects

- Passive right – main obligation of the controller
- Transparency vs “black box society” in the ages of AI
- What does it contain?
- How is it implemented in practice? From traditional privacy notice to dashboards, layers, icons, just-in-time notification, specific features of smart devices/mobile phones
- Timing
- Processing for different purposes: need to update privacy notice within a reasonable period of time and compatibility test under art. 6 (4) GDPR
- Distinguish between art. 13 and 14 of the GDPR
- Relevant case law: Bara - C-201/14; Fashion ID - C-40/17; Ryneš - C-212/13



- Ancillary to right to information, enhancing transparency and facilitating control
- Based on a request of a data subject
- Distinction between the right to access one’s own personal data and the right to request access to public information
- What does it contain?
- Relevant case law: YS - C-141/12; Nowak - C-434/16; Österreichische Post - C-154/21; Österreichische Datenschutzbehörde and CRIF - C-487/21

Key aspects

Right to rectification

- Accuracy principle
- Rectification of false/inaccurate data and right to have incomplete personal data completed
- Mechanisms to request and, if applicable, obtain free of charge rectification of personal data

Right to erasure ('right to be forgotten')

- Inspired by Google Spain – C-131/12
- Restraint applicability – withdraw of the consent, data no longer necessary for the pursuit purpose.
- Relationship with freedom of expression
- Erasure of data of all sources and storing environments
- Notification of the controllers processing personal data to erase any links to, or copies or replications of those personal data

Right to restriction

- Temporary limitation of the processing of personal data pending the granting of such rights
- Alternative right for the data subject to choose to exercise instead of right of erasure
- The right to restriction of processing grants the data subject the right to be informed by the controller before restriction is lifted

Key aspects

Right to object

- Two forms:
  - the general right to object (based on data subjects' particular situation), and
  - the right to object to marketing (unconditional right)
- Burden of proof of compelling legitimate grounds for the processing lies with the controller
- Strong connection between withdrawal of consent, the right to object and the right of erasure
- Special transparency rule – explicitly brought to the attention of the data subject and presented clearly and separately from any other information

Right to portability

Two forms:

- The right to receive their own personal data, which they have provided to a controller, in a structured, commonly used, and machine-readable format, and
- The right to transmit the data to another controller without hindrance from the controller

Limits of the right to data personability:

- Data must be "provided by" the data subject (distinction between observed data and data actively and knowingly provided by the data subject – included and, inferred and derived data – excluded)
- The right also only applies where the individual has either consented to the personal data processing or where the information is processed pursuant to a contract
- The right applies to processing carried out by automated means

Key aspects

Right not to be subject to automated individual decision-making, including profiling

- Decision adopted exclusively automated – no human intervention
- Specific rights:
  - to obtain explanations with respect to the logic used,
  - to express his/her position,
  - to challenge the decision, and
  - to obtain human intervention
- Limited legal grounds
- Is it sufficient in terms of AI and developed technology?

The Italian data protection authority - Garante announced, on 12 April 2023, that OpenAI, L.L.C., which manages ChatGPT, will have until 30 April 2023 to comply with the Garante's requirements and thus obtain a halt of the temporary ban on OpenAI to process the personal data of Italian data subjects, so that ChatGPT will be available once again from Italy.

Why?

- Lack of transparency and the necessity to provide a thorough information notice
- Invalid legal basis used – requirement to remove the references to contractual execution and to replace it with either consent on legitimate interest
- Additional measures to ensure DSAR - a set of additional measures concern the availability of tools to enable data subjects, including non-users, to obtain rectification of their personal data as generated incorrectly by the service, or else to have those data erased if rectification was found to be technically unfeasible
- Implementation of an age gating system to filter users with ages below 13 as well as users aged 13 to 18 for whom no consent is available by the holders of parental authority

Key aspects

Garante authorises OpenAI to reinstate ChatGPT

How?

- expanded the information provided to EU users and non-users;
- amended and clarified several mechanisms and deployed solutions to enable users and non-users to exercise their rights, such as the right to opt-out of processing of personal data for training of algorithms; and
- added, in a dedicated page reserved to Italian registered users, a button that allows the same to confirm that they are at least 18 years of age prior to gaining access to the service, or alternatively that they are aged above 13 and have obtained parental consent

Practical to be considered in implementation

Privacy notice – How? When ? How long? Where?

Timeline to response to requests from data subjects? – Term of response 1/2/3 months & related exceptions - unfounded/excessive requests

Refusal to response – lack of identification or other related exceptions - unfounded/excessive requests

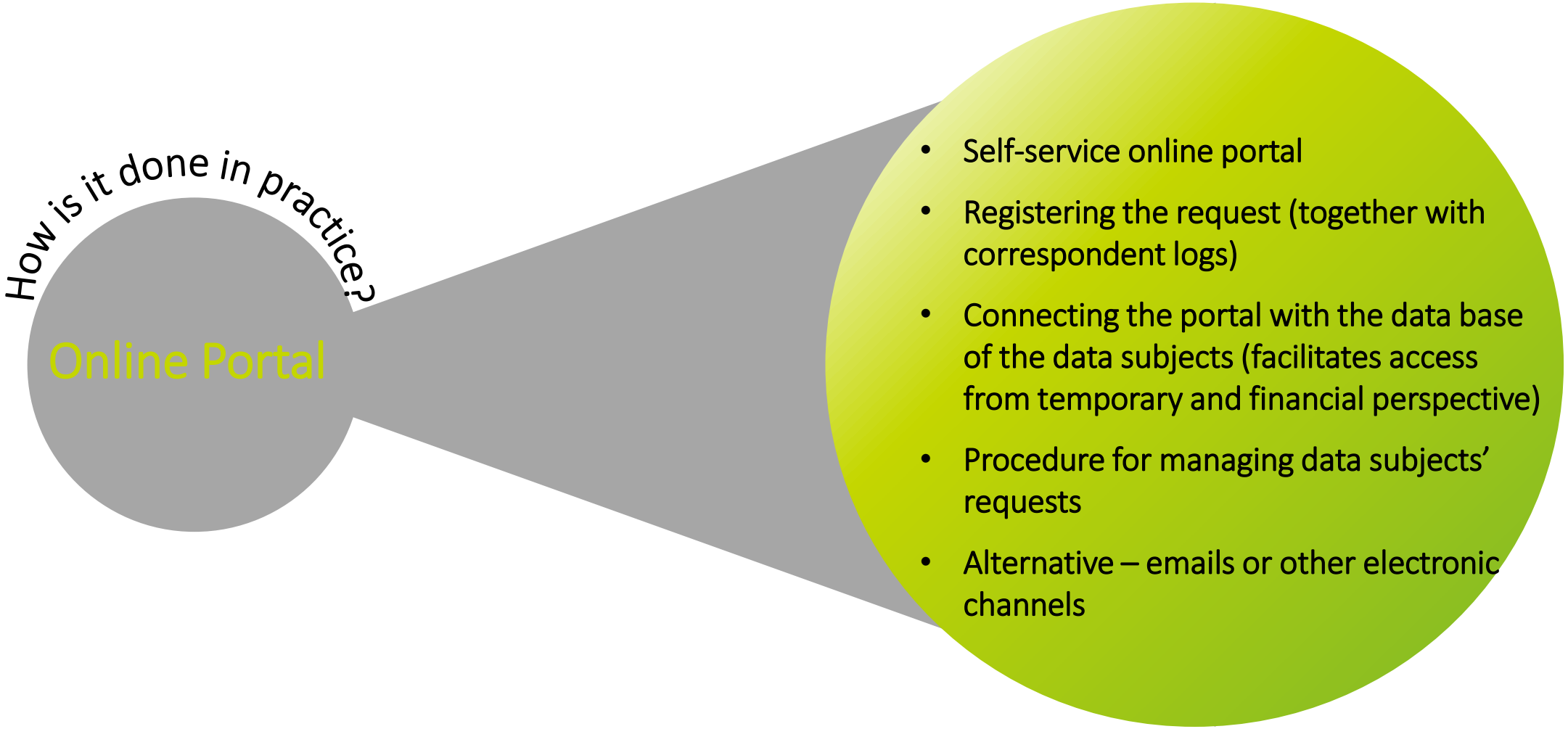
Reasonable measures to verify the identity of the data subjects – what is reasonable ?

Free vs costs in responses

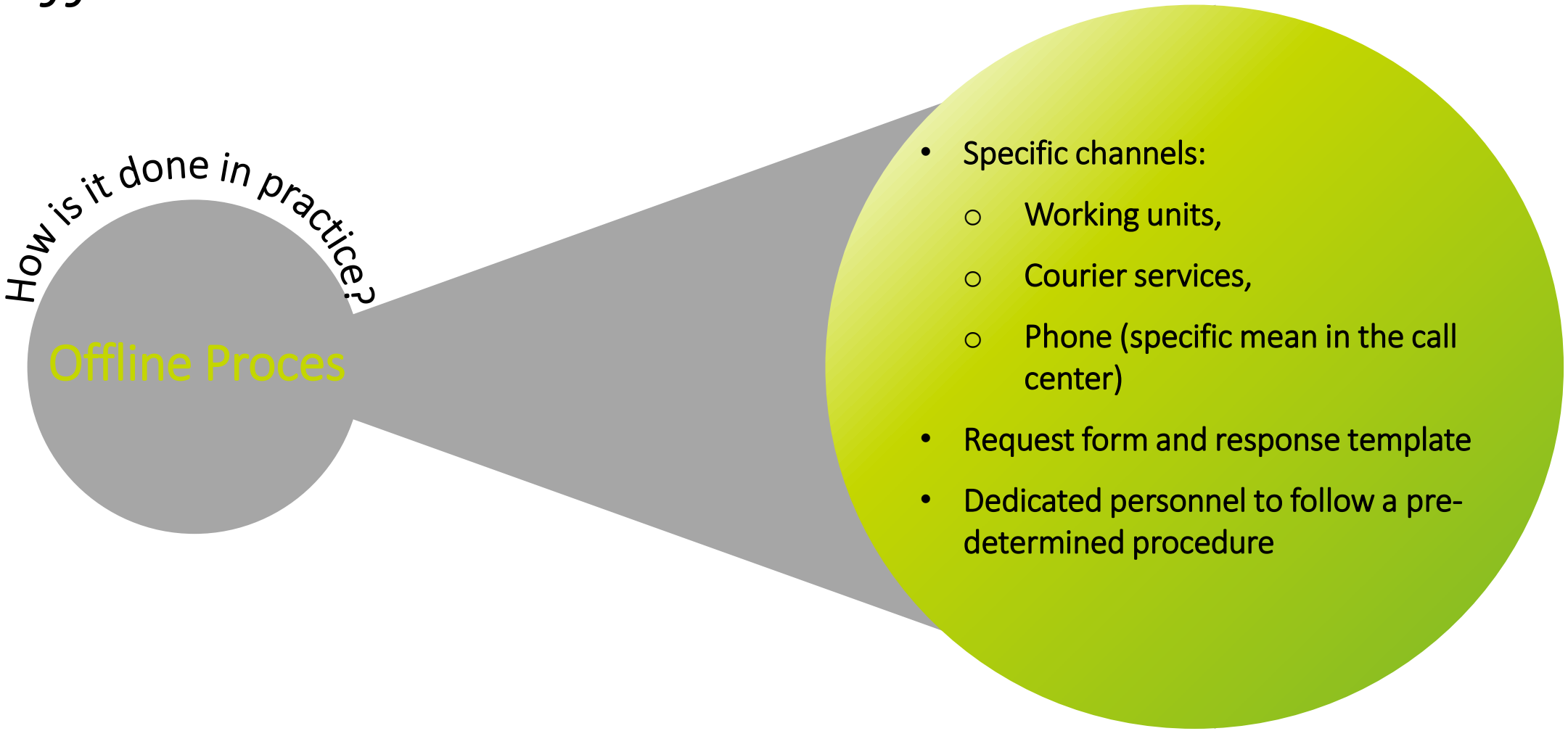
Clear & easy to understand responses

Potential request of additional information

Means to provide access for data subjects *Online*



Means to provide access for data subjects *Offline*



Speaker

Silvia Axinescu
Senior Managing Associate
maxinescu@reff-associates.ro
+40 730 585 837

THANK YOU!

Questions?

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

Principles relating to processing of personal data

Cristina Radu

Bucharest, 5 May 2023

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

INTRODUCTION

Prior protection of personal data

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

”Right to respect for private and family life

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

INTRODUCTION

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

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

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

INTRODUCTION

3. Purpose Specification Principle

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

4. Use Limitation Principle

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

a) with the consent of the data subject; or

b) by the authority of law.

INTRODUCTION

5. Security Safeguards Principle

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

6. Openness Principle

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

7. Individual Participation Principle

An individual should have the right:

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

INTRODUCTION

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

8.Accountability Principle

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

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

INTRODUCTION

➢**Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995** ***on the protection of individuals with regard to the processing of personal data and on the free movement of such data***

"PRINCIPLES RELATING TO DATA QUALITY
Article 6
1. Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

INTRODUCTION

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

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

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

- the **Regulation (EU) 2016/679 of the European Parliament and of the Council** *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (***GDPR)*** adopted on 27th of April 2016.

Article 5 - **Principles relating to processing of personal data**

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

Comparison between the Directive and the GDPR

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

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

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

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

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

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

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

1. Lawfulness, fairness and transparency

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

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

Lawfulness

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

Fairness

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

1. Lawfulness, fairness and transparency

Transparency

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

2. Purpose limitation

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

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

2. Purpose limitation

- The controller must determine the purposes-if the obligations regarding the documentation and transparency are observed, there are high chances to observe also the obligation to determine and specify the purposes. The purpose must be presented within the documentation kept as an obligation on the evidence of the processing operation and also be presented within the informing notice for the data subject. The data subject must be informed on the purpose of processing their personal data. Note: not any description of the purpose or informing on such transform an illegitimate processing into a legitimate one

- The GDPR does not forbid the use of the personal data for another purpose compatible with the initial one as long as the subject is informed and if a consent was given, to obtain their new consent

- what is an incompatible purpose? In order to determine this it needs to be analyzed the relation between the initial and new purpose, the nature of the personal data, the consequences of this new processing and if there are adequate guarantees (pseudonymisation) (ex. A doctor discloses his patients list to his daughter, who owns a travel agency for the latter to send them travel offers for spa recovery treatment)

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

3. Data minimization

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

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

4. Accuracy

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

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

4. Accuracy

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

- The controller must take reasonable measures to ensure that the personal data are accurate and otherwise, the inaccurate data are erased or rectified without undue delay

- The controller shall ensure the correction, the supplementation, update or the erasure of the inaccurate or incomplete personal data.

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

5. Storage limitation

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

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

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

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

5. Storage limitation

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

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

Some personal data cannot be erased at the decision of the controller, but observing some legal mandatory terms, ex. fiscal documents need to be kept for a longer period, as a legal obligation.
From the moment the data are not necessary for the processing purpose, these need to be either subject to anonymization or to erasure.

6. Integrity and confidentiality

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

The milestone of the GDPR – the controllers must ensure the protection of the personal data against external risks (cyber attacks) as well as internal risks (accidental losses, accidental erasure)
The novelty is that the GDPR transforms the integrity and confidentiality into a principle, not only an obligation as per the Data Protection Directive.

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

6. Integrity and confidentiality

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

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

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

7. Accountability

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

Based on the Directive the accountability was an implicit requirement of data protection law; currently, in the GDPR it has become a cornerstone of effective personal data protection. The principle ensures that throughout the processing, the controllers take responsibility for correspondingly observing all the principles of data protection, including the security and confidentiality of the personal data they process. The controllers need to implement adequate technical and organizational measures to guarantee and demonstrate that they comply with all the principles for data processing.
As per the Cambridge Dictionary - *accountability = the fact of being responsible for what you do and able to give a satisfactory reason for it, or the degree to which this happens; responsibility = something that it is your job or duty to deal with.*

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

7. Accountability

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

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

7. Accountability

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

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

7. Accountability

(ii) Demonstrate the compliance

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

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

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

7. Accountability

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

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

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

7. Accountability

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

7. Accountability

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

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

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

CONCLUSION

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

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

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

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

THANK YOU FOR YOUR ATTENTION!

MULȚUMESC PENTRU ATENȚIE!

Cristina Radu

Partner

MONOLIT Legal & Tax

Cristina.radu@monolit.ro

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

Dimitris Anastasopoulos

Bucharest, 5 May 2023

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

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

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.".*

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?

→ 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. […]".*

II. The main provisions of Directive EE2016/80

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.

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.

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.*

- ***(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

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."*.

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

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!

LAWYERS

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

Data subject's consent

Razvan Nicolae Popescu

Bucharest, 5 May 2023

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

Consent – notion – legal ground

Article 6 par.. 1 (a) of GDPR provides: „Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;"

Article 9 par. 2 (a) of GDPR provides: "the data subject has given explicit **consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject."

Article 22 par. 2 (c) of GDPR provides: "Paragraph 1 shall not apply if the decision: is based on the data subject's explicit **consent**."

Article 49 par. 1 (a) of GDPR provides: "In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: 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".

Conditions of consent

- Informed
- Free
- Clear affirmative
- Specific
- Possibility of withdrawal

Examples / Documents registered with the fiscal authority

“Declaration regarding the processing of personal data: I, the undersigned, ..., with personal number (CNP) ....., born on....., in ....., domiciled in (village, commune, town, city.) .....street ....., no. ....., building ....., entrance ....., apartment ....., County ....., holder of ID card series ....., no. ....., issued by ....., on....., hereby express my consent regarding the use and processing of personal data, according to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data to the National Fiscal Administration Agency ”.

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Examples / Petitions to the fiscal authority

“Your personal data is necessary for the request you wish to submit through the Contact Form to be resolved by the central tax authority.

Data may be disclosed to recipients or third parties only in accordance with EU law or with domestic law.

According to the provisions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) you have the right to access, rectification, erasure of personal data, the right to restrict processing, the right to object processing, the right to withdraw your consent at any time, as well as the right to file a complaint with the National Supervisory Authority for Personal Data Processing. You can exercise these rights through a request submitted in person or sent by post to the headquarters of the central fiscal authorities or by electronic means of remote transmission.

If you do not want to fill in all personal data, please use alternative channels of communication with ANAF representatives. I agree to the processing of personal data: Only after receiving the consent will it be possible to actually complete the form.”

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Examples / Documents registered with the Trade Register

Annex IX Processing of personal data

“The personal data entered in this application and in the documents submitted in support of it are registered with the trade register in accordance with the legal provisions regarding the activity/attributions/functions of the trade register and are processed in compliance with the legal provisions regarding the protection of natural persons regarding the processing personal data and free movement of such data. The documents subject to the legal obligation to be published in the Official Gazette of Romania, Part IV / VII or on the ONRC website/online service portal shall be published in submitted/transmitted form. This section represents information regarding the provisions related to the processing of the personal data of the persons who are included in the application/the documents submitted to the trade register in support of it and I agree that the personal data will be processed for the purpose of solving this application”.

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Examples / ANCPI

“By completing and signing this request, I give my consent to the processing of personal data by ANCPI/OCPI/CNC for the purpose of solving the request. Data can be communicated by ANCPI/OCPI/CNC only to recipients authorized by laws, including police bodies, prosecutors' offices, courts or other public authorities, in accordance with the law. Your personal data is kept by ANCPI/OCPI/CNC in accordance with the legal provisions regarding the archiving of documents.”

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a clear affirmative indication of will? / Does the consent fulfill the condition of being clear affirmative ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Examples / Ministry of Justice

REQUEST FOR PUBLIC INTEREST INFORMATION- According to L 544/2001

“The personal data requested from you through this application will only be processed for the purpose of processing and solving your request. The Ministry of Justice guarantees the security of data processing and their archiving in accordance with the legal provisions in force.

The Ministry of Justice is obliged to administer in safe conditions and only for the specified purposes, the personal data provided by the persons who will be registered in the electronic payment system. The purpose of data collection is to register the user in the system and automatically process his/her requests, as well as for the correct registration of receipts. Refusal to provide the requested data determines the impossibility of using the system. The person whose personal data is provided benefits from the right to be informed, the right to access, to intervene on the data, the right not to be subject to an individual decision and the right to refer to court. At the same time, the person has the right to object to the processing of personal data concerning him/her and to request the erasure of the data. To exercise these rights, a request can be sent to the administrator dpo@just.ro I agree that the Ministry of Justice processes this personal data “.

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a clear affirmative indication of will? / Does the consent fulfill the condition of being clear affirmative ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Examples / Documents drawn up by notaries public

Standard contractual clauses

“In accordance with the provisions of Regulation no. 679/27.04.2016 relating to the protection with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC and the Law of Notaries Public and no. 36/ 1995 republished, we declare that we agree with the processing of personal data in order to have the notarial deed drawn up and with the provision of information related to personal data and the content of the notarial deed to the competent authorities, at their request “.

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a clear affirmative indication of will? / Does the consent fulfill the condition of being clear affirmative ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Examples / National Union of Bailiffs

“Consent regarding the processing of personal data

By sending petitions or any documents containing your personal data by email, to any of the addresses @executori.ro, or by post, to the postal address at the UNEJ headquarters, you express your consent so that we can use your personal data, for the purposes specified in the correspondence.

For the purpose of resolving petitions/complaints or any other requests submitted by you, your data could be transmitted to the bailiff, to the Bailiff's Chamber or to any state institution exercising state authority, insofar as they have legal powers in receiving such data and in strict accordance with the applicable legal provisions.

The period of data retention. We will retain your data until the request is resolved.

The right to complain. If you have any complaints about our use of your data, which we have not been able to resolve, you can contact the National Authority for the Protection of Personal Data, according to the instructions on the website of this institution www.dataprotection.ro ”.

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a clear affirmative indication of will? / Does the consent fulfill the condition of being clear affirmative ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Examples / National Union of Bailiffs 2

“We inform you that your personal data is processed by UNEJ based on your freely expressed consent, in the user registration section, if you are a Bailiff, or on the submission of forms, if you are a Citizen.

With this consent, you agree that we process the following personal data:

The personal data entered by you in the UNEJ applications or in the portal licitatii.executori.ro;

We inform you that, at any time, you have the right to withdraw your consent regarding the processing of your data, without affecting the legality of the processing carried out on the basis of the consent before its withdrawal. Withdrawal of consent is done by completing the relevant form in the GDPR section of the licitatii.executori.ro portal or by sending an email to gdpr@executori.ro.

In this situation, your personal data will be erased from our records and any processing thereof will cease. “

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a clear affirmative indication of will? / Does the consent fulfill the condition of being clear affirmative ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Examples / Private domain

Processing of employee data

Video surveillance (employees, shopping center visitors, etc.)

Contracting lawyers

Calling on the services of a bailiff

Biological samples for medical tests

Hospitalization in a private hospital

Calling on the services of a car service

Debatable aspects:

- Is there a prior information? / Does the consent fulfill the condition of being informed ?
- Is there a real possibility of choice? / Does the consent fulfill the condition of being free ?
- Is there a clear affirmative indication of will? / Does the consent fulfill the condition of being clear affirmative ?
- Is there a certain granularity? / Does the consent fulfill the condition of being specific ?
- Does the withdrawal of consent produce legal effects? / Can the consent be effectively withdrawn ?

Informed consent

Article 4 (11) of GDPR provides: „For the purposes of this Regulation: 11. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;”

Paragraph 32 of the GDPR preamble provides: „Consent should be given by a clear affirmative act establishing a freely given, specific, **informed** and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement”

Paragraph 42 of the GDPR preamble provides: „For consent to be informed, the data subject should **be aware at least** of the identity of the controller and the purposes of the processing for which the personal data are intended.”

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Interpretation and application

According to opinion no. 8/2001 of the Working Party, the notion of informed consent assumes that : „… the employee must have information regarding the necessary processing in accordance with art. 10 and 11 ”

According to opinion no. 15/2011 of the Working Party, the notion of informed consent assumes that: „To be valid, consent must be informed. This implies that all the necessary information must be given at the moment the consent is requested, and that this should address the substantive aspects of the processing that the consent is intended to legitimise. This would normally cover the elements of information listed in Article 10 of the Directive, but will also depend on when, and the circumstances in which, consent is requested. This means in practice that "consent by the data subject (must be) based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, in particular those specified in Articles 10 and 11 of the Directive, such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject.”

According to the guidelines on consent from 2018 issued by the Working Party, the notion of informed consent implies that: „Providing information to data subjects before obtaining their consent is essential to allow them to make informed decisions, to understand the aspects they express agreement for and, for example, exercise the right to withdraw consent. If the controller fails to provide accessible information, user control becomes illusory, and consent will not constitute a valid basis for processing. In order for a consent to be informed, it is necessary for the data subject to be informed about certain elements that are essential to make a choice.

Thus, WP 29 considers that at least the following information is necessary to obtain a valid consent: (i) the identity of the controller, (ii) the purpose of each processing operation for which consent is requested, (iii) the type of data that will be collected and used, (iv) the existence of the right to withdraw consent, (v) information regarding the use of data for the automated decision-making process in accordance with Article 22 paragraph (2) letter (c), if applicable, (vi) regarding the possible risks related to data transfers due to the lack of a decision regarding the adequacy of the level of protection and adequate guarantees, as described in Article 46.”

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Free consent

Article 7 par. 4 of GDPR provides: „When assessing whether consent is **freely** given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract"

Article 4 (11) of GDPR provides: „For the purposes of this Regulation: 11. 'consent' of the data subject means any **freely given**, specific, informed and unambiguous **indication** of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

Paragraph 32 of GDPR preamble provides: „Consent should be given by a clear affirmative act establishing a **freely given**, specific, informed and unambiguous **indication** of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement"

Paragraph 42 of GDPR preamble provides: „Consent should not be regarded as **freely given** if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment"

Paragraph 43 of GDPR preamble provides: „In order to ensure that consent is **freely given**, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance"

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Interpretation and application

In Opinion no. 8/2001 the Working Party considered that: „The Working Party is of the opinion that, where data processing is necessary and represents an inevitable consequence of employment relationships, an employer is mistaken when it tries to justify this processing on the basis of consent. The use of consent by the employer should be limited to cases where the employee has real freedom of choice and can withdraw his/her consent without being prejudiced."

In Opinion no. 15/2011 the Working Party considered that : „An example of the above is provided by the case where the data subject is under the jurisdiction / influence of the data controller, such as an employment relationship. In this example, although the data subject may not always be dependent on the data controller, due to the nature of the relationship or special circumstances, he/she may fear that he/she may be treated differently if he/she does not accept the data processing".

In the 2018 guidelines on consent, the Working Party considered that: "A power imbalance also occurs in the context of employment relations. Considering the dependence resulting from the relationship between employer and employee, it is unlikely that the data subject can refuse to give his/her consent to his/her employer for data processing without facing the fear or the real risk of negative consequences as a result of a refusal. It is unlikely that an employee will be able to freely respond to a request for consent from their employer, for example to activate monitoring systems such as surveillance cameras in the workplace, or to complete assessment forms, without feeling the pressure to consent."

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Clear affirmative consent

Article 6 par. 1 (a) of GDPR provides: „Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;"

Article 7 par. 1 of GDPR provides: „Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."

Article 4 (11) of GDPR provides: „For the purposes of this Regulation: 11. 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of personal data relating to him or her"

Paragraph 32 of GDPR preamble provides: „Consent should be given by a **clear affirmative act** establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement"

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Interpretation and application

In opinion no. 15/2011 the Working Party considered that: “For the consent to be unequivocal, the procedure to seek and give the consent must remove any kind of doubts regarding the intention of the data subject to issue the consent. In other words, the manifestation of will by which the data subject expresses his/her consent must not leave room for ambiguity regarding his/her intention. If there is reasonable doubt about the person’s intent, there is ambiguity.”

In the 2018 consent guidelines, the Working Party considered that: “Also, a controller must be aware of the fact that consent cannot be obtained through the same action that the conclusion of a contract is agreed or the general terms and conditions of a service are accepted. Blanket acceptance of the general terms and conditions cannot be considered as an unequivocal action of consenting to the use of personal data.”

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Specific consent

Article 6 par. 1 (a) of GDPR provides: „Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes”

Article 7 par. 1 of GDPR provides: „Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data”

Article 4 pct. 11 of GDPR provides: „For the purposes of this Regulation: 11. ‘consent’ of the data subject means any freely given, **specific**, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;”

Paragraph 32 of GDPR preamble provides: „Consent should be given by a clear affirmative act establishing a freely given, **specific**, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. (…) Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.”

Paragraph 43 of GDPR preamble provides: „Consent is presumed not to be freely given if it does not allow **separate** consent to be given to different personal data processing operations despite it being appropriate in the individual case…”

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Interpretation and application

In Opinion no. 15/2011 the Working Party considered that: “To be valid, consent must be specific. In other words, blanket consent without specifying the exact purpose of the processing is not acceptable. To be specific, consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing. It cannot apply to an open-ended set of processing activities. This means in other words that the context in which consent applies is limited. Consent must be given in relation to the different aspects of the processing, clearly identified. It includes notably which data are processed and for which purposes. ”

Within the 2018 consent guidelines, the Working Party considered that : „Consent mechanisms must be detailed not only to fulfill the “free” requirement, but also to satisfy the “specific” condition. This means that a controller that requires consent for a number of different purposes should offer a separate option for each purpose in order to allow users to give specific consent for specific purposes. Finally, controllers should provide specific information, together with each separate request for consent, regarding the data that is processed for each purpose, so that data subjects are aware of the impact of the different options available to them.”

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Withdrawal of consent

Article 6 par. 1 (a) of GDPR provides: „Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;"

Article 7 par. 1 of GDPR provides: „Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data"

Article 7 par. 3 of GDPR provides: „The data subject shall have the **right to withdraw** his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent"

Article 4 pct. 11 of GDPR provides: „For the purposes of this Regulation: 11. 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;"

Paragraph 42 of GDPR preamble provides: „Consent should not be regarded as freely given if the data subject has no genuine or free choice or **is unable to refuse or withdraw consent** without detriment."

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Interpretation and application

By opinion no. 15/2011 the Working Party considered that: “The notion of control is also related to the fact that the data subject should be able to withdraw his/her consent. The withdrawal is not retroactive, but should, in principle, prevent any further processing of the person's data by the controller”

Through the 2018 Consent Guidelines, the Working Party considered that: “The requirement to easily withdraw consent is described as a necessary aspect of valid consent in the GDPR. If the right of withdrawal does not comply with GDPR requirements, then the controller's consent mechanism does not comply with GDPR. As mentioned in section 3.1 regarding the condition of informed consent, the controller must inform the data subject of the right to withdraw consent before the effective granting of consent, in accordance with Article 7 paragraph (3) of the GDPR. Moreover, as part of the obligation of transparency, the controller must inform the data subjects about the way to exercise their rights.”

Examples / Documents registered with the fiscal authority ; Examples / Petitions to the fiscal authority ; Examples / Documents registered with the Trade Register ; Examples / ANCPI ; Examples / Ministry of Justice ; Examples / Documents drawn up by public notaries ; Examples / National Union of Bailiffs ; National Union of Bailiffs 2 ; Examples / Private domain

Effects and limitations

Consent, by itself, is not sufficient to ensure a legal processing of personal data

Any processing of personal data must, on the one hand, meet all the requirements provided by art. 5 par. 1 of the GDPR (“Principles related to the processing of personal data”), and on the other hand, to be based on at least one of the legal bases provided by art. 6 par. 1 of the GDPR (“Lawfulness of processing”).

Since the consent of the data subject is only one of the legal grounds that can justify data processing, this, by itself, is not sufficient to ensure the lawfulness of the processing by a controller, the latter being required to comply with the conditions provided by art. 5 par. 1 of the GDPR.

In the same sense is the opinion of the Working Party. (2018 Consent Guidelines issued by the Working Party, page 4)

The working party has already shown that there may be situations in which the processing of personal data is considered illegal due to the fact that, although the employee gave his consent regarding data processing, the data collected by the employer were excessive (our note thus violating the condition provided by art. 5 par. 1 letter c of the GDPR regarding the collection of only data limited to what is necessary for the purposes of the processing to be achieved). (Opinion no. 8/2001 of the Working Party, page 18)

The Working Party has also confirmed on another occasion that the mere granting of consent by the data subject will never legitimise the controller to collect excessive personal data in relation to the purpose for which they are collected/processed. (Opinion no. 15/2011 of the Working Party, page 7; 2018 Consent Guidelines issued by the Working Party, page 4).

In certain situations, data controllers resort to requesting the consent of the data subject in order to transfer responsibility for the data to them (e.g. we disclosed the data / transmitted the data because the client agreed, etc.).

Such a practice is illegal, considering the fact that, as we have seen before, the mere existence of the consent of the data subject does not grant the data controller the freedom to process the data in any way.

Moreover, the Working Party emphasized the fact that the existence of consent should not be understood as determining the exoneration of the controller from processing the data in accordance with the provisions of art. 5 of the GDPR (our note former art. 6 of the Directive). (Opinion no. 15/2011 of the Working Party, page 9)

Conclusions

Consent is only one of the legal grounds that allow the processing of personal data.

It is recommended that this legal ground be used only in cases where there are no other legal grounds for data processing.

Whenever consent is used, the controller must fulfill all legal conditions (informed, free, clear affirmative, specific, etc.)

Even to the extent that all the conditions imposed by law will be fulfilled, the consent will not, by itself, be sufficient to ensure a legal processing of the data, being necessary for the data controllers to comply with all the principles of data processing.

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

Data controller and processor

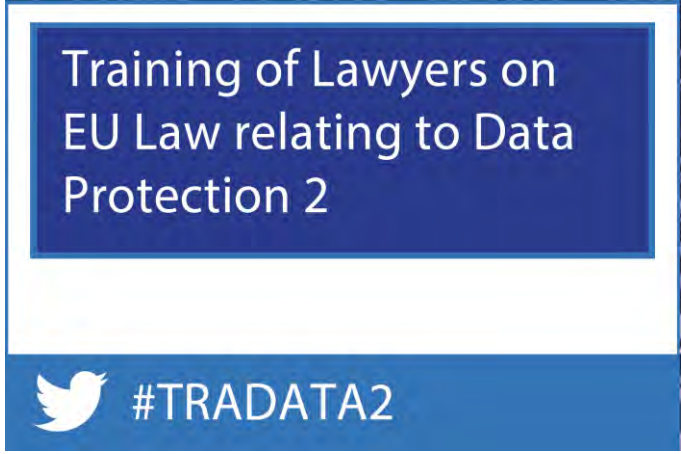
Silvia Axinescu

Bucharest, 5 May 2023

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

Data controller and processor

Silvia Axinescu, lawyer Romanian Bar National Association



- EU Regulation 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)
  - The concepts of controller, joint controller and processor – crucial role
  - Assessment and qualification
  - Relationship between the parties

What is personal data?

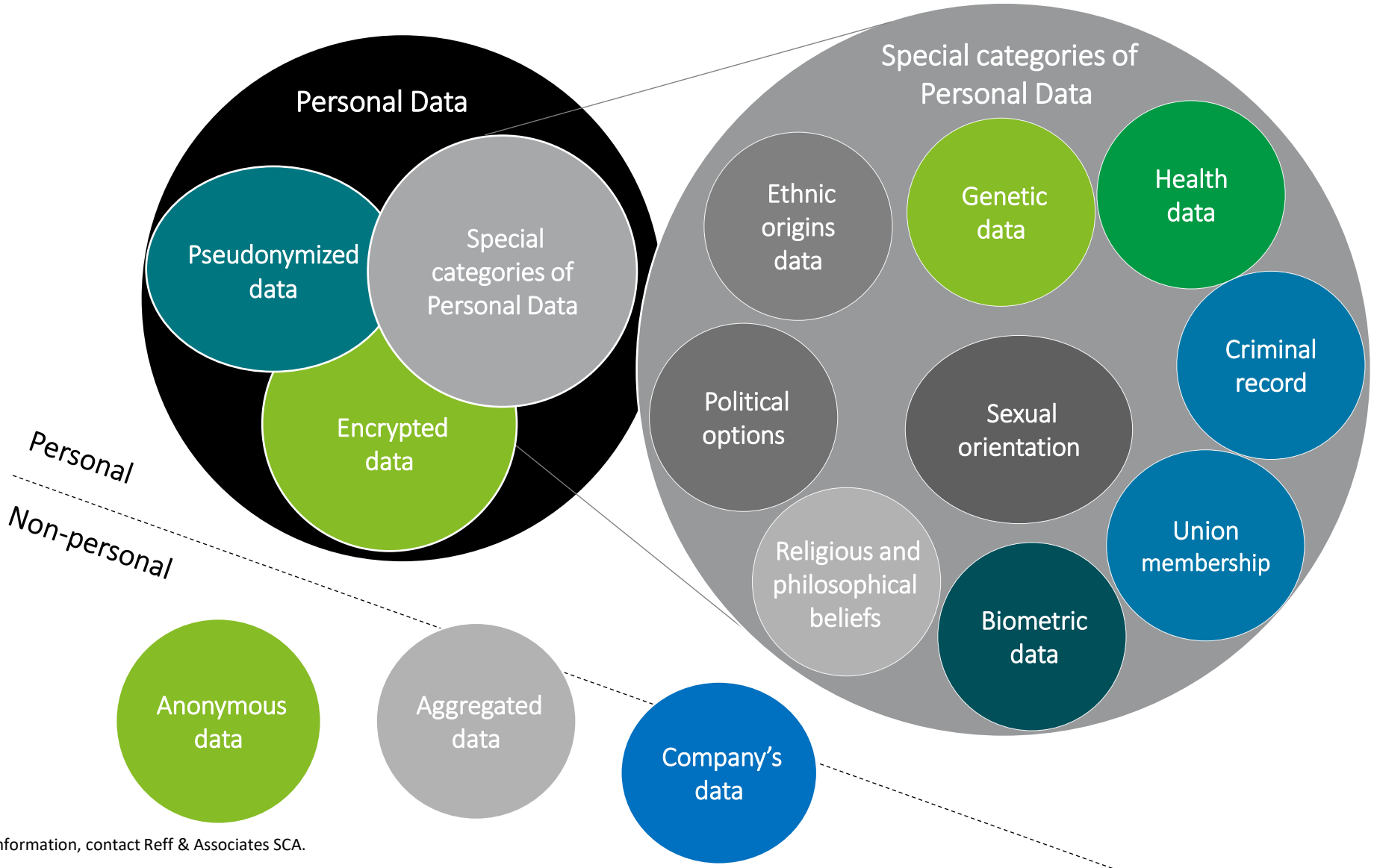
Definition

'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

Data which may be processed

- e-mail
- image
- voice
- citizenship
- signature
- sex
- name and surname
- full name of family members
- address (home/residence)
- profession/job title
- training/diplomas/studies
- date and place of birth
- data on owned assets
- pension file no.
- telephone / fax
- nickname / alias
- geolocation data
- data from driver's license / certificate of registration
- physical / anthropometric data
- habits / preferences / behavior
- economic & financial situation
- family status
- military status
- civil status data
- bank data

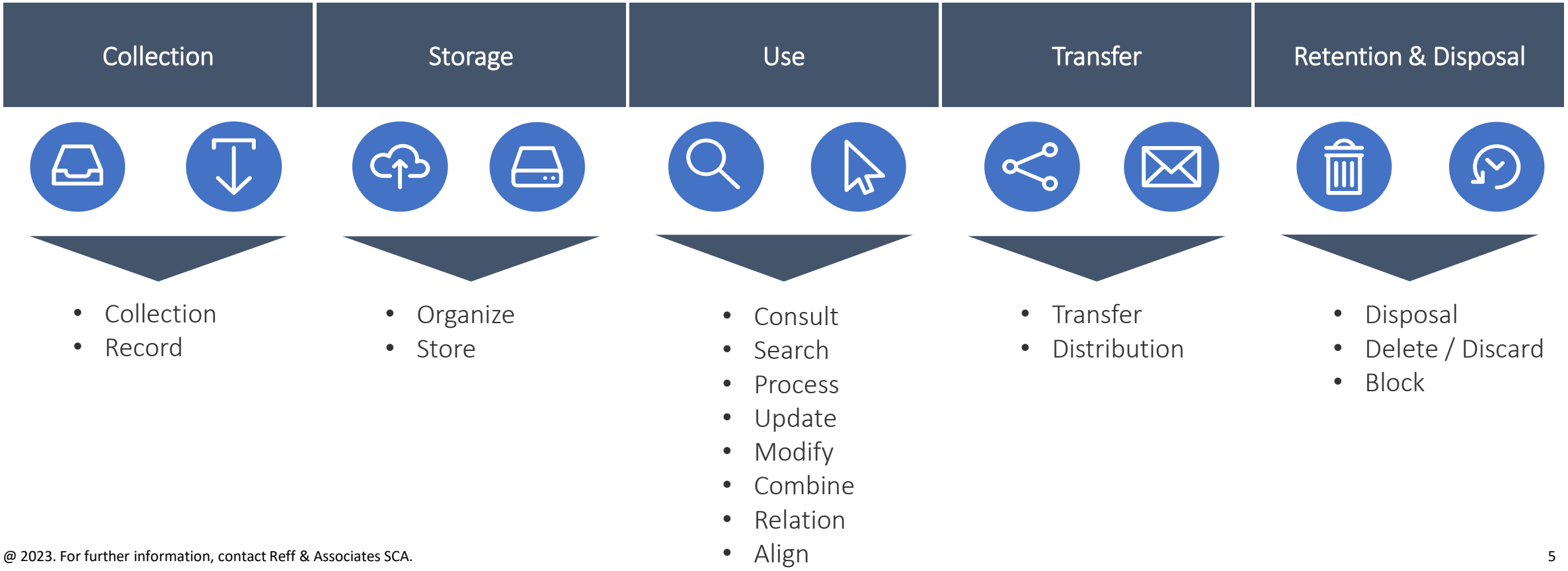
Types of personal data



Processing

Processing: any operation performed upon personal data (collecting, recording, organization, use, disclosure by transmission, alignment or combination, erasure or destruction)

Personal Data lifecycle



Concepts

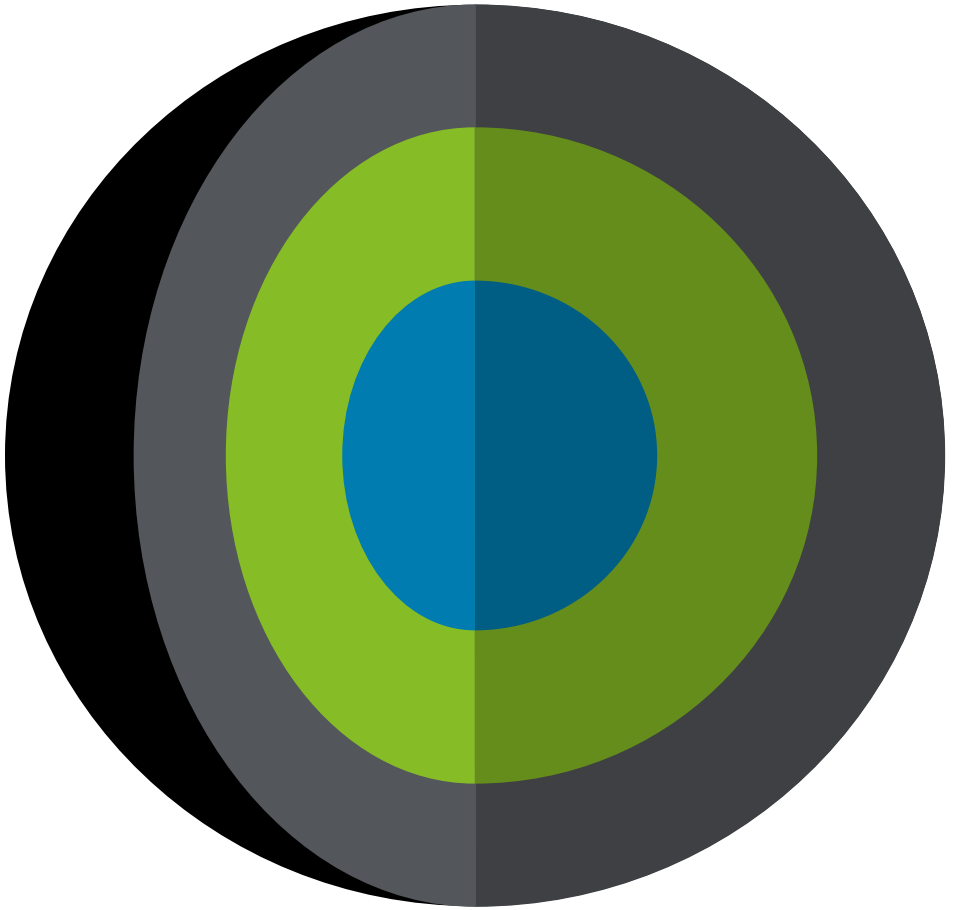
Controller

Natural or legal person, public authority, agency or other body

Alone or jointly with others

Determines the purposes and means of processing (control)

- ✓ Why? (purposes)
- ✓ How? (means)
- ✓ What data?
- ✓ How long? (retention)
- ✓ Where? (storage and data transfers)
- ✓ By whom?



Controller

Examples

1. Regulated professions
2. Debt collection agencies
3. Meal ticket companies
4. Financial institutions
5. Service providers intermediated by travel agencies on the basis of customer contracts, such as hotels, car rental companies, airlines, bus companies, insurance companies
6. Payment services providers
7. Fb fan page holders (see Judgment in Case C-210/16)

Controller

Observing data protection principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality

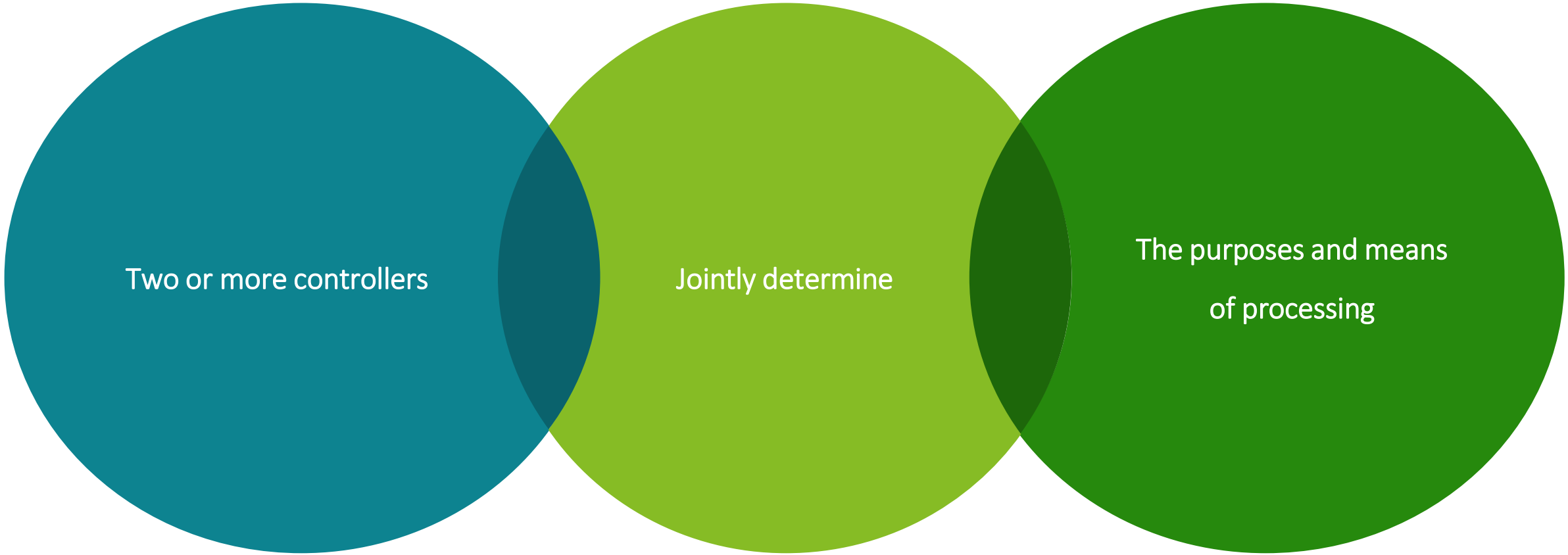
Identify a legitimate basis for processing

Compliance with individuals' rights

- Transparency obligations (part of the right to be informed)
- Other rights under the GDPR

Concepts

Joint controllers



Joint controllers

Examples

Fb “Like” button – Case C-40/17

Jehovah’s Witnesses Community – Case C-25/17

Concepts

Processor

1

Natural or legal person, public authority, agency or other body

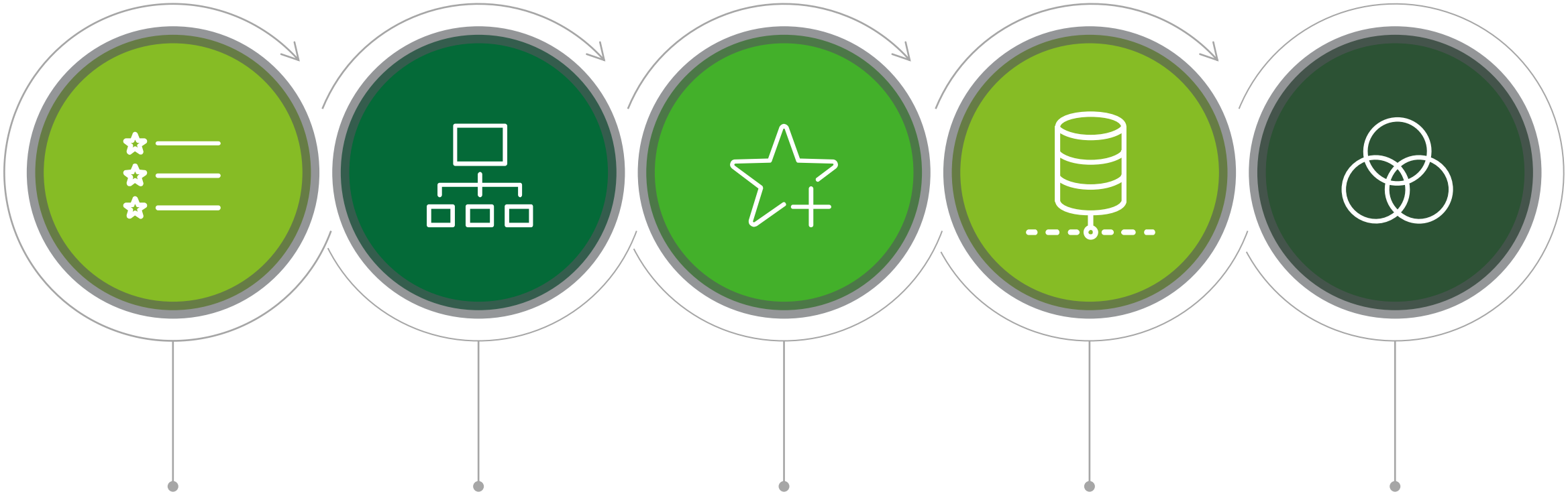
2

Processes personal data on behalf of the controller

- written instructions only
- provides services to a controller
- protects personal data
- demonstrates compliance

Processor

Examples



Cloud services providers

Call center providers

Physical security companies

IT providers

Hosting services providers

A processor that determines the purposes and the essential means of the processing may be a controller in fact (Art. 28 (10) from the GDPR)

- The active role of a processor in making certain decisions about the processing (unless it does not exceed the scope of what was envisaged by the agreement with the client)
- Use of data beyond the scope pursuit by the client
- The determination of the technical and organizational means of processing vs. the determination of the other issues related to the means of processing

To be assessed considering:

- The contractual provisions related to the distribution of rights and obligations
- The degree of detail pertaining to the instructions granted to the processor by the controller
- Visibility portrayed to the individual

Engagement of processors

Choose reliable processors (offering “adequate guarantees”)

Pre-contractual due diligence

- ✓ Processor’s data protection knowledge
- ✓ Under investigation?
- ✓ Data protection framework

Evaluate the activity of the processors

Frame the relationship in a contract

Processor

Agreement with the client

Contract in place containing:

- Subject matter, duration and nature of the processing
- Types of personal data and categories of data subjects
- Obligations and rights of the client
- The processor's responsibilities

Minimum clauses to be included pursuant to the GDPR, such as:

- Vest employees to ensure confidentiality
- Assist the controller in responding to requests for exercising data subjects' rights
- Delete or return all personal data to the client at the latter's request
- What liability bears the processor for failure to include these mandatory requirements?

Other important clauses

- Liability
- Monitoring the execution of the obligations by the controller
- Timeline and procedure for execution of certain obligations

Processor

Other contractual aspects

01 Clarification of the responsibilities of the processor to notify the client in the event of any data breach which affects the client's data.

02 Obligation of the processor to provide a list of locations in which the data may be processed (if multiple locations).

03 The controller's rights to monitor and the processor' corresponding obligations to cooperate.

04 It should be contractually fixed that the processor must inform the client about relevant changes concerning the respective services such as the implementation of additional functions.

Clarifying roles and responsibilities of the parties under the GDPR

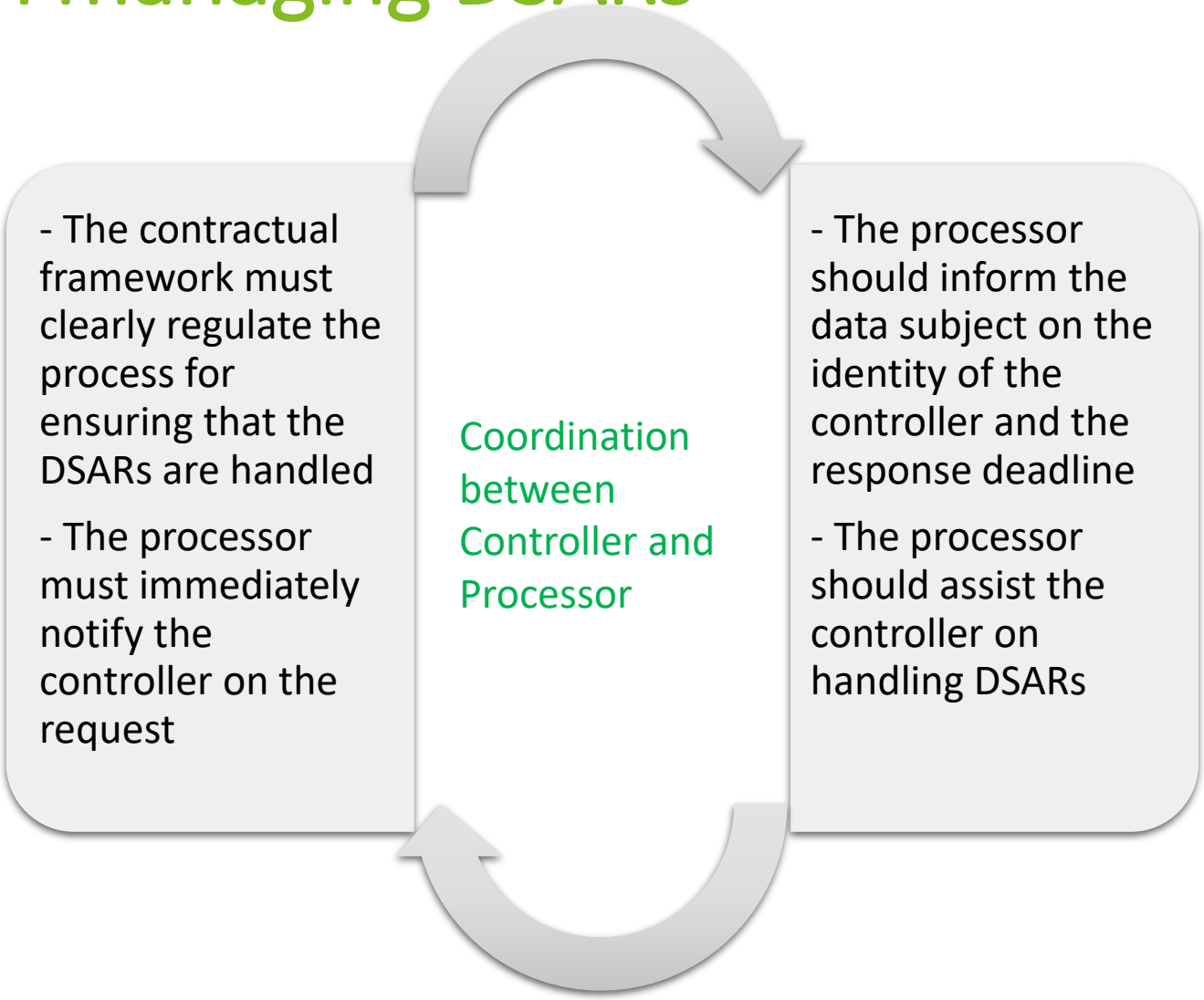
Necessity to clarify the legal basis of the processing – rests with the client (controller)

- Legitimate interest (security, monitoring)
- Consent (i.e. marketing)

Compliance with individuals' rights rests with the client (controller) but can be contractually passed (processor)

- Transparency obligations (as part of the right to be informed)
- Solving individuals' requests
- To be assessed under the agreement with the client

Challenges in managing DSARs



Security measures

Personal data breach documentation

❑ Documenting breaches by the controller – internal register of breaches

No	Sample content
1	Details regarding the breach
2	Causes of the breach
3	Personal data affected
4	Consequences of the breach
5	Remedial action taken
6	Reasoning for decisions taken to respond
7	Justification for not notifying (if applicable)
8	Reasons for notification delay (if applicable)
9	Proof of communication (if applicable)

❑ Processor obligations

- Controller retains the overall responsibility for data protection
- Processor enables the controller to comply with its obligations
- Processor becomes aware of breach to data it processes – notify the controller without undue delay
- Further information related to the breach – provided in phases
- Report details of the incident to each controller
- Processor could make the notification on behalf of the controller

Speaker

Silvia Axinescu
Senior Managing Associate
maxinescu@reff-associates.ro
+40 730 585 837

THANK YOU!

Questions?