KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

EU Data Protection Law: Rights and Remedies

Elora Fernandes

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Academy of European Law. Neither the European Union nor the granting authority can be held responsible for them.

Class overview

Data subject rights of the GDPR

Data subject rights and EU fundamental rights

Exercising data subject rights

Enforcing data subject rights

Data subject rights of the GDPR

- No oficial definition.
- Individual rights granted to data subjects to control the processing of their personal data.
- To be exercised in the first place against the controller (individual, company, public authority…).
- They are also enforceable.

Right to withdraw consent (Art. 7(3))

Right of Access (Art. 15)

Right to Rectification (Art. 16)

Right to Erasure (Art. 17)

Right to Restriction of Processing (Art. 18)

Right to Data Portability (Art. 20)

Right to Object (Art. 21)

Right to obtain human intervention, express their point of view and contest automated decision-making (Art. 22(3)

Right of access

- Directly linked with the principle of transparency
- Two main functions:
  - Enhancing transparency: provides a second layer of information to data subjects
  - Facilitating control: with the right of access, a data subject can exercise other rights (such as rectify information)
- Bundle of four rights:
  - Obtain confirmation of processing
  - Access to personal data;
  - Access to individualized information (such as the purposes for processing or categories of data);
  - Copy of personal data undergoing processing.

Right to rectification

- The right to rectification reflects the principle of accuracy and grants more control to data subjects in relation to the quality of data.
- It includes the correction of inaccurate personal data and the right to have incompleted data completed.
- Who should determine the level of accuracy that is required? Do data subjects have the right to provide innacurate information (for example in social media)?
- AI systems and infered data.

Right to Erasure (Right to be Forgotten)

- Not applicable to all situations – specific grounds should be identified:
  - Lack of basis for the processing (personal data are no longer necessary; consent had been withdrawn; personal data are unlawfully processed).
  - Consequence of the right to object.
  - Compliance with a legal obligation.
  - Collection of data when the data subject was a child, and consent has been given by the holder of parental responsibility.
- Importance of balancing data protection with other rights such as freedom of expression and freedom of the press.

Right to Object

- It is aligned with the fairness principle.
- It refers to the data subject's ability to request that the processing activities stop according to his or her particular situation.
- Unconditional right to object when data are processed for direct marketing.
- General right to object
  - Data must have been processed based on the necessity for a task in the public interest or in the exercise of official authority vested in the controller, or on the legitimate interests of the controller (art. 6(1)(e) and (f)).
  - Demands a balance test of its own (beyond the ex-ante balancing test performed when processing based on 6(1)(e)), as compelling legitimate grounds for the processing must be demonstrated (such as exercising defence of legal claims).

Right to obtain human intervention, express their point of view and contest automated decision-making

- Art. 22 – “Right” not to be subject to a decision based solely on automated processing which produces legal effects concerning him or her or similarly significantly affects him or her.
  - Worded as a right, but has been understood as a prohibition by DPAs and this understanding has been confirmed by the CJEU.
- Not applicable if the decision is necessary for a contract, authorised by Union or MS law or based on consent.
  - Need to implement safeguards such as human intervention, expression of the data subject’s point of view and contest the decision.
- Aligned to the principle of fairness and the need to have control over automated decision making.

Right to obtain human intervention, express their point of view and contest automated decision-making

- What fully automated decision means? – Need for real influence of a person and meaningful human oversight.
- “Legal effects”
- “Similarly significantly affects” - effects must have a degree of significance that is roughly equivalent to that of legal effects

Data subject rights and EU fundamental rights

Data protection and data subject rights as a means to protect other fundamental rights

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 8 – EU Charter

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

But not only…

- Privacy – Article 7, Charter
- Freedom of thought, conscience and religion – Article 10, Charter
- Freedom of expression and information – Article 11, Charter
- Freedom of assembly and of association – Article 12, Charter
- Non-discrimination – Article 21, Charter
- The rights of the child – Article 24, Charter
- Effective Judicial Protection – Article 47, Charter
- …

Data subject rights are not absolute

Article 52

Scope of guaranteed rights

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

2. Rights recognised by this Charter which are based on the Community Treaties or the Treaty on European Union shall be exercised under the conditions and within the limits defined by those Treaties.

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

Data subject rights are not absolute

Scope of data subject right is inherently limited (e.g. right to erasure – Art. 17(3) GDPR)

Member State of Union Law restrictions – Art. 23 GDPR

Abuse of Rights – Art. 12(5) GDPR

Exercising data subject rights

Contingencies of data subject rights: Transparency Requirements (Articles 13 and 14, GDPR)

Information	Direct	Indirect
The purposes of the processing	✓	✓
The legal basis of the processing	✓	✓
The identity of the controller	✓	✓
The contact details of the controller	✓	✓
The contact details of the DPO (if there is a DPO)	✓	✓
The recipients or categories of recipients of the data	✓	✓
Information if the data will be transferred outside the European Economic Area (EEA), and where applicable: the existence or not of an adequacy decision or reference to the appropriate safeguards and how this information can be made available to data subjects	✓	✓
If the legal basis for the processing is the legitimate interests of the data controller: specific information about which legitimate interests relate to the specific processing, and about which entity pursues each legitimate interest	✓	
The categories of personal data processed		✓

Information	Direct	Indirect
The retention period or, where this is not possible, the criteria used to determine this period	✓	✓
The right to request access, erasure, rectification, restriction, objection and portability of personal data	✓	✓
The right to lodge a complaint with a data protection authority	✓	✓
If the legal basis for the processing is consent: the right to withdraw consent at any time	✓	✓
The existence of automated decision-making, relevant information about the underlying logic and the intended consequences of the processing for the data subject	✓	✓
The legitimate interest of the controller, if the processing has this legal basis		✓
The source of the personal data		✓
Whether the data subject is required to provide the personal data (by law or by contract or to enter into a contract) and what the consequences of refusing to provide the data are	✓	

Tables from EDPB Data Protection Guide for SMEs

Contingencies of data subject rights: Transparency Requirements

Information	Direct	Indirect
The purposes of the processing	✓	✓
The legal basis of the processing	✓	✓
The identity of the controller	✓	✓
The contact details of the controller	✓	✓
The contact details of the DPO (if there is a DPO)	✓	✓
The recipients or categories of recipients of the data	✓	✓
Information if the data will be transferred outside the European Economic Area (EEA), and where applicable: the existence or not of an adequacy decision or reference to the appropriate safeguards and how this information can be made available to data subjects	✓	✓
If the legal basis for the processing is the legitimate interests of the data controller: specific information about which legitimate interests relate to the specific processing, and about which entity pursues each legitimate interest	✓	
The categories of personal data processed		✓

Who is processing personal data?

Tables from EDPB Data Protection Guide for SMEs

Contingencies of data subject rights: Transparency Requirements

Information	Direct	Indirect
The purposes of the processing	✓	✓
The legal basis of the processing	✓	✓
The identity of the controller	✓	
The contact details of the controller	✓	
The contact details of the DPO (if there is a DPO)	✓	
The recipients or categories of recipients of the data	✓	
Information if the data will be transferred outside the European Economic Area (EEA), and where applicable: the existence or not of an adequacy decision or reference to the appropriate safeguards and how this information can be made available to data subjects	✓	
If the legal basis for the processing is the legitimate interests of the data controller: specific information about which legitimate interests relate to the specific processing, and about which entity pursues each legitimate interest	✓	
The categories of personal data processed		✓

Information	Direct	Indirect
The retention period or, where this is not possible, the criteria used to determine this period	✓	✓
re, rectification, ity of personal data	✓	✓
th a data protection	✓	✓
g is consent: the time	✓	✓
ion-making, derlying logic and processing for the	✓	✓
The legitimate interest of the controller, if the processing has this legal basis		✓
The source of the personal data		✓
Whether the data subject is required to provide the personal data (by law or by contract or to enter into a contract) and what the consequences of refusing to provide the data are	✓	

What personal data are collected?

Tables from EDPB Data Protection Guide for SMEs

Contingencies of data subject rights: Transparency Requirements

Information	Direct	Indirect
The purposes of the processing (Including further processing)	✓	✓
The legal basis of the processing	✓	✓
The identity of the controller	✓	
The contact details of the controller	✓	
The contact details of the DPO (if there is a DPO)	✓	
The recipients or categories of recipients of the data	✓	
Information if the data will be transferred outside the European Economic Area (EEA), and where applicable: the existence or not of an adequacy decision or reference to the appropriate safeguards and how this information can be made available to data subjects	✓	
If the legal basis for the processing is the legitimate interests of the data controller: specific information about which legitimate interests relate to the specific processing, and about which entity pursues each legitimate interest	✓	
The categories of personal data processed		✓

Information	Direct	Indirect
The retention period or, where this is not possible, the criteria used to determine this period	✓	✓
e, rectification, ty of personal data	✓	✓
h a data protection	✓	✓
g is consent: the me	✓	✓
on-making, derlying logic and processing for the	✓	✓
The legitimate interest of the controller, if the processing has this legal basis		✓
The source of the personal data		✓
Whether the data subject is required to provide the personal data (by law or by contract or to enter into a contract) and what the consequences of refusing to provide the data are	✓	

Why are personal data collected?

Tables from EDPB Data Protection Guide for SMEs

Contingencies of data subject rights: Transparency Requirements

How are personal data being processed?

Information	Direct	Indirect
The purposes of the processing		
The legal basis of the processing		
The identity of the controller		
The contact details of the controller		
The contact details of the DPO (if there is a DPO)	✓	✓
The recipients or categories of recipients of the data	✓	✓
Information if the data will be transferred outside the European Economic Area (EEA), and where applicable: the existence or not of an adequacy decision or reference to the appropriate safeguards and how this information can be made available to data subjects	✓	✓
If the legal basis for the processing is the legitimate interests of the data controller: specific information about which legitimate interests relate to the specific processing, and about which entity pursues each legitimate interest	✓	
The categories of personal data processed		✓

Information	Direct	Indirect
The retention period or, where this is not possible, the criteria used to determine this period	✓	✓
The right to request access, erasure, rectification, restriction, objection and portability of personal data	✓	✓
The right to lodge a complaint with a data protection authority	✓	✓
If the legal basis for the processing is consent: the right to withdraw consent at any time	✓	✓
The existence of automated decision-making, relevant information about the underlying logic and the intended consequences of the processing for the data subject	✓	✓
The legitimate interest of the controller, if the processing has this legal basis		✓
The source of the personal data		✓
Whether the data subject is required to provide the personal data (by law or by contract or to enter into a contract) and what the consequences of refusing to provide the data are	✓	

Tables from EDPB Data Protection Guide for SMEs

Contingencies of data subject rights: Transparency Requirements

Information	Direct	Indirect
The purposes of the processing	✓	✓
The legal basis of the processing	✓	✓
The identity of th		✓
The contact detai		✓
The contact detai		✓
The recipients or		✓
Information if the the European Eco applicable: the ex decision or refer and how this info data subjects		✓
If the legal basis for the processing is the legitimate interests of the data controller: specific information about which legitimate interests relate to the specific processing, and about which entity pursues each legitimate interest	✓	
The categories of personal data processed		✓

What are the rights of the data subject?

Information	Direct	Indirect
The retention period or, where this is not possible, the criteria used to determine this period	✓	✓
The right to request access, erasure, rectification, restriction, objection and portability of personal data	✓	✓
The right to lodge a complaint with a data protection authority	✓	✓
If the legal basis for the processing is consent: the right to withdraw consent at any time	✓	✓
The existence of automated decision-making, relevant information about the underlying logic and the intended consequences of the processing for the data subject	✓	✓
The legitimate interest of the controller, if the processing has this legal basis		✓
The source of the personal data		✓
Whether the data subject is required to provide the personal data (by law or by contract or to enter into a contract) and what the consequences of refusing to provide the data are	✓	

Tables from EDPB Data Protection Guide for SMEs

Contingencies of data subject rights: Behaviour of the Controller

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

- Article 12 is a procedural provision regulating the flow of information between controllers and data subjects, enabling the latter to more effectively exercise their rights;
- Concise, transparent, and easily accessible form (quality of information);
- Intelligible, using clear and plain language (comprehensibility) – especially important for children.

Contingencies of data subject rights: Behaviour of the Controller

Could the examples below be considered poor or good practices?

- “We may use your personal data to develop new services”;
- “We may use your personal data for research purposes;
- “We may use your personal data to offer personalised services”.

Contingencies of data subject rights: Behaviour of the Controller

Could the examples below be considered poor or good practices?

- “We may use your personal data to develop new services” (it is unclear what the “services” are or how the data will help develop them);
- “We may use your personal data for research purposes;
- “We may use your personal data to offer personalised services”.

Contingencies of data subject rights: Behaviour of the Controller

Could the examples below be considered poor or good practices?

- "We may use your personal data to develop new services" (it is unclear what the "services" are or how the data will help develop them);
- "We may use your personal data for research purposes (it is unclear what kind of "research" this refers to);
- "We may use your personal data to offer personalised services".

Contingencies of data subject rights: Behaviour of the Controller

Could the examples below be considered poor or good practices?

- "We may use your personal data to develop new services" (it is unclear what the "services" are or how the data will help develop them);
- "We may use your personal data for research purposes (it is unclear what kind of "research" this refers to);
- "We may use your personal data to offer personalised services" (it is unclear what "personalisation" entails).

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

Contingencies of data subject rights: Behaviour of the Controller

Good practices according to WP29:

- We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in ” (it is clear what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this).
- We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read” (it is clear what personalisation entails and how the interests attributed to the data subject have been identified).

Contingencies of data subject rights: Behaviour of the Controller

- Article 12 (2): controller must facilitate the exercise of data subject rights;

- Article 12 (3): controller must respond to data subject without undue delay within one month of receipt of the request, extendable to three months where necessary

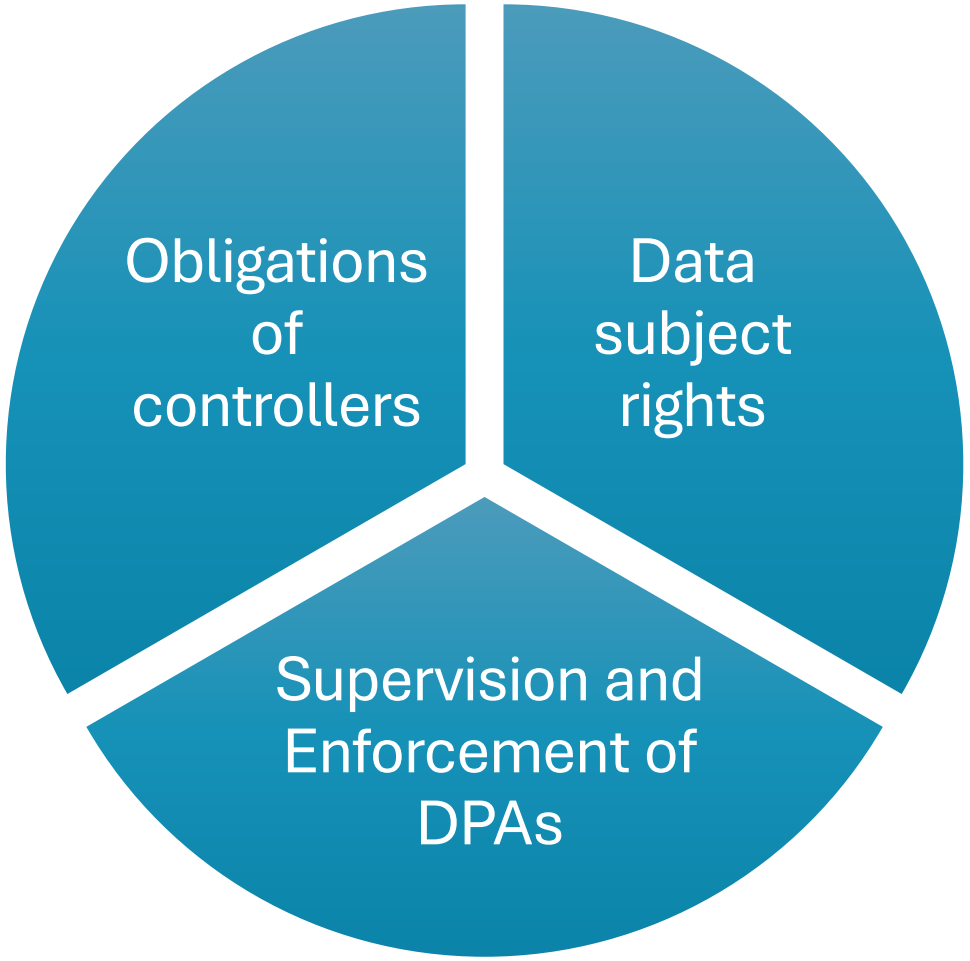
Enforcing (data subject) rights under the GDPR

Key scenarios for lodging a complaint related to data subject rights

- Failure to respond to a request (in a timely manner);
- Incomplete Response;
- Unlawful refusal to comply with the request (e.g. to access data).

Individuals can lodge a complaint with a supervisory authority (Article 77) or seek judicial remedy in court (Article 79).

Tripartite structure of the GDPR



Data Protection Authorities (DPAs)

GDPR:

Article 51

Supervisory authority

+ Article 52

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

Charter:

Article 8

Protection of personal data

3. Compliance with these rules shall be subject to control by an independent authority.

TFEU:

Article 16

(ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

Powers of DPAs (Art. 58)

- **Investigative powers** – powers to establish the facts of a case, including: orders to provide information; carry out investigations; notify controllers and processors of allenged infringements; obtain access to information and premises…
- **Corrective powers** – powers to ensure compliance with the GDPR, including: issue warnings that intended processing operations are likely to infringe the GDPR *(ex ante);* orders to bring processing operations into compliance; suspend data flows; impose bans; impose fines…
- **Authorisation and advisory powers**, including: give advise to controllers in accordance with prior consultation; issue opinions; approve of codes of conducts…
- Bring infringements of the GDPR to the attention of the judicial authorities.

Enforcement problems with GDPR

- What is wrong with the GDPR?

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679

Private enforcement of the GDPR in courts

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

+ EU's Representative Actions Directive (2020/1828)

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Thank you!

KU Leuven Centre for IT & IP Law (CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip

imec KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW