Data protection principles and data subjects’ rights in the GDPR

Spring 2018
Susanna Lindroos-Hovinheimo, Senior Lecturer, Faculty of Law
The GDPR

A few words about method, i.e.
How can claims about legal meaning be made?
Doctrinal method (lainoppi / oikeusdogmatiikka)

- Aims to interpret and systematise the law
- The traditional legal scientific method
- Done by practicing lawyers, judges and legal researchers
- Argumentation is central > the results are measured by the quality of the argumentation
- Nowadays other methods too, e.g. legal sociology, economic analysis of law etc.
Doctrinal analysis of law

- Aims at finding out the meaning of law: what does the law command?
- The results need to be argued for > reliability and replication as in other sciences.
- Results of legal research usually of two types:
  - *De lege lata*
  - *De lege ferenda*
Object of study: the GDPR

• Question: what does it say about data protection principles and the rights of data subjects
• Answers: interpretation & argumentation needed, the text does not apply itself
• This is EU law, so the argumentation needs to follow accepted practices in EU law > ultimately: the ECJ decides on the meaning of the regulation on a case-by-case basis

➢ Interpretation of EU law is a practice shaped primarily by the ECJ
Legal reasoning of the ECJ

- General rule: EU law is a system *sui generis* and must be interpreted as such.
- Systemic, contextual and teleological arguments tend to rank highest in the ECJ:s case law (see CILFIT 1982).
- Teleological arguments: the purpose of the provision to be interpreted + the aims and objectives of the legal system.
- The context in which the provision is to be interpreted varies.
- Linguistic arguments rank lowest, since, as the ECJ has itself admitted, language is a problematic argument (especially) in a multilingual legal system.
Legal reasoning of the ECJ

• Lenaerts & Gutierrez-Fons: the teleological method of interpretation plays an important role in the ECJ's legal reasoning but:

“Where the EU law provision in question is ambiguous, obscure or incomplete, all the methods of interpretation employed by the ECJ operate in a mutually reinforcing manner. A literal interpretation of an ambiguous EU law provision may be confirmed by its context and purposes. Similarly, to determine the objectives pursued by an EU law provision, the ECJ may have recourse to its drafting history and/or its normative context.”

Starting points for interpretation: which context is relevant here?

- The GDPR is part of EU fundamental rights regulation > this is the framework for interpretation
- The GDPR has aims > telos relevant for interpretation, although may be unclear or lead to contradictory results (free flow of data vs. subjects’ rights)
- The GDPR has already been interpreted by authoritative sources, see especially Article 29 Data Protection Working Party http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
- There are already some very relevant judgments from the ECJ, although they pre-date the GDPR
Art. 29 WP

• The EU’s national supervisory have been collaborating in the framework of the Article 29 Working Party.
• The European Data Protection Supervisor and the Commission are also members.
• Art. 29 WP is an advisory body > legal power limited *de jure*, if not *de facto*. It was created by the Data Protection Directive.
• As of 25 May 2018, the Article 29 Working Party will be replaced by the European Data Protection Board (EDPB).
• The EDPB will become an EU body with legal personality will have an independent secretariat > this means some changes in power and responsibility.
How to read the GDPR?

Protection of personal data is a fundamental right protected in EU law

➢ Processing of personal data is restricted

➢ The GDPR tells us on which conditions processing is allowed

➢ When processing is allowed, certain rules and principles have to be followed

➢ If not, then fines apply

(Still: the free movement of data shall not be prohibited or restricted by protection of natural persons (Article 1: aims)
Article 5: Principles relating to processing of personal data

- Article 5 puts forward a list of general principles that relate to all processing of personal data (regardless of the nature of the data or the nature of the processing)
- The list can be interpreted as closed (although the GDPR does include other articles that introduce more principles)
- Article 5 includes 10 principles:
Article 5: Principles relating to processing of personal data

1. Personal data shall be:
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
   (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’);
Article 5: Principles relating to processing of personal data

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(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’);
(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’);
Article 5: Principles relating to processing of personal data

(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’).
Article 5: Principle of accountability

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

➢ Burden of proof is with the controller.
➢ See also Article 24: controller shall implement appropriate technical and organisational measures to ensure **and to be able to demonstrate** that processing is performed in accordance with this regulation
➢ Also Article 30 (records of the controller) & Article 35 (impact assessment)
➢ More flexibility for the controllers and processors?
Additional principles in the GDPR

- Article 25: Data protection by design and by default
- Commission: The principles of data protection by design and by default create incentives for innovative solutions to address data protection issues from the start

Communication COM(2018) 43 final
Article 5: Principles relating to processing of personal data

• The principles are not new (except accountability)
• They set the tone for the whole regulation > they can be used as a dynamic measuring stock when considering infringements
• They can be used as a tool to interpret the case-by-case meaning of the other articles of the GDPR (systemic interpretation)
• They emphasise that the processor needs to be able to show that the principles have been followed
Principle of lawfulness

• See preamble 40:

In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
Article 6: Lawfulness of processing

1. 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;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
Article 6: Lawfulness of processing

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
Article 6: Lawfulness of processing

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
Article 6: Lawfulness of processing

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) [legal obligation and public interest] by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

(Chapter IX: e.g. freedom of expression, public access to documents, id numbers, scientific purposes etc.)
Article 6: Lawfulness of processing

3. The basis for the processing referred to in point (c) and (e) shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller… etc.
Article 6: Lawfulness of processing

Article 6(4) Purposes of national safety etc (as defined Article 23): Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, the controller shall take into account e.g.:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.
Special categories of data >
different criteria for lawfulness

Article 9: racial or ethnic origin, political or religious beliefs, sexual orientation, data relating to health etc.

• These are sensitive data.
• Preamble 51: "Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms."
• The article includes a list of data that are to be regarded sensitive. The list is closed but the definitions open.
• Stricter grounds for processing: it is prima facie prohibited (paragraph 1).
Sensitive data

Processing is allowed only by consent, if not regulation to the contrary:

"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"
Sensitive data

Processing is also allowed under certain conditions in the field of employment and social security and social protection law, when it is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent etc.
Sensitive data

Processing is allowed when it relates to personal data which are manifestly made public by the data subject, or processing is necessary for legal claims or in courts, or processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law etc.
Sensitive data

- In several issues, the GDPR leaves room for national legislation, e.g. on processing of sensitive data
- See e.g. preamble 10 that refers to this: even though harmonisation goals, the GDPR does not exclude MS law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.
Rights of the data subject

Article 12: Rights to ensure the exercise of the rights of the data subject

Articles 13, 14: Rights to information

Article 15: Right of access

Article 16: Right to rectification

Article 17: Right to erasure "right to be forgotten"
Rights of the data subject

Article 18: Right to restriction of processing
Article 20: Data portability
Article 21: Right to object
Article 22: Right not to be subject to a decision based solely on automated processing
Article 77, 78, 79: Rights to remedies
Article 82: Right to compensation
Rights of the data subject

- The rights correspond with the principles.
- They give detail and content to the principles.
- They also correspond with the responsibilities of the data controller (and the processor).
- In essence, these rights define the various aspects of the right to protection of personal data in the EU.
- In practice it is not one right, it is many.
What should Member States do?

• Even though the GDPR is a regulation, it requires MS to implement legislation to complement it.
• How? On a regulatory level Member States are bound by:
  Article 8 of the Charter on the one hand and Article 16(2) TFEU (national legislation cannot impinge on the free flow of personal data within the EU) on the other.
• They are also bound by the case law of the EU Court.
• See HE 9/2018 vp
Who says what the GDPR says?

- The interpretation of the Regulation is the task of European courts (also MS courts are European).
- Commission is strict: the national legislator is not allowed to copy the text of the GDPR unless it’s absolutely necessary, nor interpret it, nor add additional conditions > harmonisation goals & restriction of MS powers

Questions?