

SUMMARY SHEETS : ARTICLE 8 ECHFR

“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.”*


Content and scope of the article

Article 8 EChFR acknowledges data protection as an autonomous fundamental right. Regardless of the specifics of a particular matter, any processing of personal data by itself can be considered an interference. Therefore, **the protection established by the Charter is not dependent on the private or sensitive nature of the data or the existence of inconvenience to its owner.** There are intrinsic differences between the right to privacy and the right to data protection, with the latter being understood as a modern take on privacy, adapted for the digital age.

Besides reproducing the wording of Article 8 (1) of the Charter, Article 16 TFEU also establishes a legal basis for the adoption of EU secondary legislation. Among the most relevant instruments on data protection currently, the **General Data Protection Regulation (GDPR)** and the Law Enforcement Directive should be highlighted. The main purpose of the GDPR is to adapt to several technological developments. The Law Enforcement Directive established the data protection rules and principles that govern personal data processing to prevent, investigate, detect, and prosecute criminal offences, or execute criminal penalties.

Article 5 GDPR enounces the principles that govern data processing in the EU, such as:

- The lawfulness, fairness, and transparency of the data processing.
- The purpose limitation So the data must be collected for specified, explicit and legitimate purposes. No other processing is allowed except in certain cases that are not incompatible with the initial purpose.
- The data minimization. Thus, data cannot be processed when it is not justified by the purpose.
- The accuracy. Inaccurate data must be erased or deleted without delay.
- The storage limitation. The personal data retention is allowed for no longer than is necessary.
- The integrity and confidentiality. The appropriated security technical measures to ensure unauthorized, or unlawful processing must be taken.



All these principles have a translation into concrete rights developed in arts. 12-22 GDPR, such as, the rights of information, access, rectification, and erasure. Article 5(2) GDPR also refers to the principle of accountability, which translates to the obligation to the controller for ensuring data protection according the GDPR. In fact, any data processor must follow the principles enshrined in Article 5 GDPR, and they form a solid basis for litigation.

Furthermore, in *Maximillian Schrems v. Data Protection Commissioner* (CJEU C-362/14) the CJEU noted that Article 8 (3) EChFR and Article 16 (2) TFEU establish independent supervisory authorities that are “[...] *an essential component of the protection of individuals with regard to the processing of personal data.*” And reaffirmed that when a complaint is lodged with a national supervisory authority, the authority must examine the complaint with diligence.

Limitation of the right

The right of data protection is not absolute and may be subject to certain limitations. Indeed, it may be limited by the concurrence with some other Charter right or due to a general interest. And according to Article 52 (1), limitations are admissible only if they:

- 1) are provided for by law,
- 2) respect the essence of the right to data protection,
- 3) are proportionate,
- 4) are necessary, and
- 5) meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

CJEU Case Law

CJEU Judgement, *Google Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317.

Key words: Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Extent of that operator’s obligations and of the data subject’s rights

CJEU Judgement, *Digital Rights Ireland and Seitlinger and Others*, C-293/12, ECLI:EU:C:2014:238.

Key words: Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services

CJEU Judgment, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijke- boer*, C-553/07, ECLI:EU:C:2009:293.

Key words: Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Respect for private life - Erasure of data - Right of access to data

and to information on the recipients of data - Time-limit on the exercise of the right to access.

CJEU Judgement, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

Key words: Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services.

Case Judgement, *Ligue des droits humains v Conseil des ministres*, C-817/19, ECLI:EU:C:2022:491.

Key words: Regulation (EU) 2016/679 – Directive (EU) 2016/681 – Use of PNR data of air passengers of flights operated between the European Union and third countries – Power to include data of air passengers of flights operated within the European Union – Automated processing of that data – Retention period – Fight against terrorist offences and serious crime.

Highlights

Practical Relevance of Article 8

1. Dual Enforcement Mechanisms:

- Lawyers can pursue **extrajudicial remedies** by engaging with National Data Protection Authorities (DPAs) in Member States, which oversee compliance with data protection laws. The effectiveness of this approach depends on the proactivity and resources of each DPA.
- **Judicial remedies** are also available for direct challenges under Article 8 and related data protection regulations, such as the GDPR.

2. Collective Remedies:

- The General Data Protection Regulation (GDPR) permits joint actions for infringements, enabling consumer groups or representative bodies to take collective legal action.
- **Key Reference:** The CJEU's judgment in *Meta Platforms Ireland* (C-319/20) confirms the possibility of consumer representation in data protection cases.
- Lawyers must consider the criteria established under Directive (EU) 2020/1828 on representative actions when pursuing collective remedies.

3. Intersection with Other Rights:

- Article 8 works in tandem with **Article 7 (Right to Private and Family Life)** to protect against breaches of privacy. However, it is important to distinguish between the two:
 - **Article 7:** Provides broader protection against interference in private life but is subject to public interest exceptions.

- **Article 8:** Regulates any processing of personal data, regardless of its impact on privacy, and is subject to strict compliance with data protection rules.

Examples of Application

1. **Challenging Excessive Data Collection:**
 - Use Article 8 to argue against unnecessary or disproportionate data collection practices by public or private entities, citing GDPR principles such as data minimization and purpose limitation.
2. **Cross-Border Data Transfers:**
 - In cases involving international data transfers, invoke Article 8 and GDPR provisions to assess the adequacy of data protection in the receiving country.
3. **Data Breaches:**
 - Represent individuals or groups in cases involving security failures leading to personal data breaches, demonstrating non-compliance with GDPR obligations.

Correspondence with other European/International instruments

- European Convention on Human Rights, Article 8 – Right to respect for private and family life
- Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data
- OECD, Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data

Further readings

Kranenborg, Herke; “Article 8, Protection of Personal Data”, in Peers, Steve, Hervey, Tamara, Kenner, Jeff and Ward, Angela (Eds.), *The EU Charter of Fundamental Rights*, Hart, 2014, pp. 223-266.