BALANCING OF RIGHTS OF DATA SUBJECTS AND DATA CONTROLLERS UNDER THE GDPR

International Business Law

Master's thesis

Author:

PRERNA BHUSHAN

Supervisor:

Didem Polad

11.11.2025

Helsinki

Title: Balancing of Rights of Data Subjects and Data Controllers under the GDPR

Author: PRERNA BHUSHAN

Month and year: NOVEMBER 2025

Number of pages: 88 pages

Keywords: GDPR, DATA SUBJECT, DATA CONTROLLER, ANALYSIS, OBLIGATIONS, PROPORTIONALITY, NECESSITY, FUNDAMENTAL RIGHTS, RECTIFICATION, ACCESS, ERASURE, OBJECT, TRANSPARENCY

Abstract:

The current thesis analyses the balance between the rights of data subjects and the obligations of data controllers under the GDPR. As data becomes increasingly central to economic and social activity, the GDPR seeks to harmonize protection across member states, ensuring individuals retain control over their personal data while organizations are held to high standards of accountability and transparency. The GDPR does not curtail processing of data but regulates it. The thesis is based around the principles of proportionality, necessity, and respect for fundamental rights, which serve as interpretative guides for GDPR provisions. Data controllers are tasked with implementing comprehensive measures ranging from risk assessments and record-keeping to technical safeguards to comply with requirements of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. Simultaneously, data subjects are empowered with rights to access, rectify, object to, and erase their personal data, creating practical obligations for controllers to facilitate these rights. Through doctrinal analysis and case studies, the thesis demonstrates how the GDPR operationalizes balancing in both legal and practical terms. While the regulation aspires to achieve equilibrium, the reality is that data controllers particularly small and medium-sized enterprises face significant operational and financial burdens. The rights of data subjects are strong but not absolute. The thesis concludes that while the GDPR provides a strong legal foundation for balancing competing interests, the practical implementation often results in disproportionate responsibilities for controllers. To foster a more equitable balance, the study recommends enhanced practical guidance, ongoing dialogue between regulators and organizations, and adaptive strategies to address emerging challenges in the evolving digital landscape.

List of Abbreviations

Abbreviation	Full Form
GDPR	General Data Protection Regulation
EU	European Union
ECHR	European Convention on Human Rights
CFR	Charter of Fundamental Rights (of the EU)
TFEU	Treaty on the Functioning of the European Union
ECJ / CJEU	European Court of Justice / Court of Justice of the European Union
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
DPbDD	Data Protection by Design and Default
DPIA	Data Protection Impact Assessment
ROP	Records of Processing
DPA	Data Protection Authority
WP29	Article 29 Working Party
ICO	Information Commissioner's Office (UK)
AML	Anti Money Laundering
TIA	Transfer Impact Assessment
SME	Small and Medium-sized Enterprises
FR	Fundamental Rights
Rec.	Recital (of the GDPR)
Art.	Article (of the GDPR or other legislation)

TABLE OF CONTENTS

I INTRODUCTION

1.1 Background

In a world where data is more valuable than oil for all businesses, the European Union (EU), in order to safeguard, monitor and ensure legitimate use of personal data worked on the EU Digital framework. Data fuels the digital economy, much like oil powered the industrial age, it's a valuable resource driving innovation, growth, and competitive advantage. The EU had created a Digital Agenda 2020 for Europe in 2010, with the aim to deliver sustainable economic and social benefits from a digital single market based on fast and ultra-fast internet and interoperable applications.[1] The idea was to maximize social and economic potential of the ICT and reduce the risks arising from fragmented digital markets, lack of interoperability, rising cybercrimes and risk of low trust in networks, lack of digital literacy and skills. The focus was to have a data economy that is trustworthy, safe and economically viable to use. To ensure that trust, economic viability *etc*. is in place, a regulation ensuring uniform protection in whole Europe was much needed.

This vision of gave rise to multiple regulations and paved way EU Digital Regulatory Framework which includes the The General Data Protection regulation (GDPR)[2], The Data Act[3], The Digital Services Act[4], The Data governance Act[5] *et. Al.* The regulations are the pillars to upload the control of individuals on their personal data while aiming for free flow of data and creating a robust digital economy. Data sharing is central to Europe's digital vision. As the EU promotes data-driven innovation, it seeks to maintain a balance with privacy, security, ethics and safety, while looking into the use and sharing of non-personal data for new technologies and business paradigms.[6]

---

[1] European Commission, *A Digital Agenda for Europe: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* COM(2010) 245 final, Brussels, 19 May 2010, 1

[2] Regulation (EU) 2016/679 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 and on the free movement of such data [2016] OJ L119/1

[3] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data (Data Act) [2023] OJ L 2023/2854

[4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1

[5] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act) [2022] OJ L152/1

[6] European Parliament, 'Digital Agenda for Europe' (Fact Sheets on the European Union) <https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe> accessed 2 June 2025.

The GDPR is seen as the cornerstone of the EU digital policy building as it establishes a comprehensive and unified legal framework for personal data protection across all EU member states, replacing fragmented national laws and gives individuals more control over their personal data, while imposing strict obligations on organizations that process such data, ensuring accountability and transparency. The aim was to to support the consistent application of the data protection framework in relation to new technologies, in order to support innovation and technological developments.[7]

The GDPR came in to force in 2018. The GDPR aims at harmonising the data protection laws across the European Union and provide a minimum level of safeguard to processing of personal data. It gives individuals more control over the use of their personal data with their data in the digital transition. It is also contributing to foster trustworthy innovation, notably through a risk-based approach and principles such as data protection by design and by default.[8] It has equipped national data protection authorities with stronger and harmonized enforcement powers, and has established a new governance system among the data protection authorities and has created a level playing field for all companies operating in the EU market, regardless of where they are establish, ensures the free flow of data within the EU, facilitates safe international data transfers and has become a reference point at global level.[9] The GDPR intends to protect the rights of data subjects by regulating the processing of data and also by placing several obligations on data controllers while processing data. The GDPR has laid down obligations on data controllers along with providing rights to data subjects, and in this era where there is an increasing reliance of personal data to provide services by the organisation , a conflicting interest is created in terms of Individual's right to Privacy and organisations obligations that are imposed by provisions of the GDPR.

In other words, the obligations on data controllers not only come from the principles laid down in GDPR for controller but it also arises from the direct effect of rights granted to data subject. The GDPR under Article 5 has principles all of which create obligations on the data controllers. These

[7] European Commission, *Second Report on the Application of the General Data Protection Regulation*, COM(2024) 482 final, Communication from the Commission to the European Parliament and the Council, Brussels, 25 July 2024

[8] European Commission, 'Antitrust: Commission fines Apple €1.1 billion for anti-competitive practices in the distribution of Apple Pay' IP/20/1163, 16 June 2020, 1 <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_1163/IP_20_1163_EN.pdf> accessed 24 March 2025.

[9] Ibid at page 3

principles are also affirmed under other articles of the GDPR, meaning the principle of transparency forms the basis of art. 13 and art. 14 of the GDPR, whereas accountability principle is the elaborated under art. 24 and art. 25, and the principles of integrity and confidentiality can be found under art. 32 of the GDPR. These principles are based on article 5 of the Convention 108 and were also a part of Directive 95/46. The principles laid down under Art. 5 are the main restriction for processing legal data in line with the requirements of the regulation. Transparency is an overarching obligation under the GDPR applying to three central areas:[10]

(1) the provision of information on data subjects related to fair processing.

(2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and

(3) how data controllers facilitate the exercise by data subjects of their rights.

Lawfulness of processing has six bases under Art. 6 of the GDPR. This is in correlation to the general restriction on processing of personal data, also specified under Art. 8(2) of the Charter. The principle of lawfulness does not mean that processing which violates any administrative provision of the GDPR or any other law (environmental laws, tax law, employment laws), makes the processing not 'lawful' within the meaning of the GDPR, as this would for example trigger the fine under Article 83(5) GDPR.[11] The principle of fairness is interpreted in the light of requirement set under Art. 8 of the Charter on Fundamental Rights and is closely associated with the principle of proportionality. The principle of fairness is made to capture the situations where the processing does not violate the black letter of law. The principles of accountability, accuracy, data minimization, purpose limitation *etc*. ensure that the processing of personal data is limited and the data controller justifies the processing.

The rights of data subjects, acknowledged under chapter 3 of the GDPR, begins with stating obligation for data controllers under art. 12. The objective of art. 12 is to mitigate the risks of longh, incomprehensible, ambiguous privacy policies often shared by data controllers.The Chapter at the outset outlines the appropriate measures that a data controller should take to facilitate the

[10] Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679*, WP260 rev.01, adopted on 29 November 2017, revised and adopted on 11 April 2018

[11] GDPRhub, 'Article 5 GDPR – Principles relating to processing of personal data' (GDPRhub) <https://gdprhub.eu/Article_5_GDPR> accessed 15 May 2025.

rights acknowledged therein. It lays down a proactive duty on the controller to take reasonable actions to meet the requests by data subjects while exercising their rights under the GDPR.

The GDPR, speaks of the modalities that the controller should undertake to meet the requests of data subjects. On one hand, the Chapter acknolwedges the rights of the data subjects, but on another the exercise of the rights add more obligations on data controllers to create modalities to meet the requirements. The falter or non performace can lead to heavy fines on data controllers. Data controllers are expected to embrace these obligations as a duty *in lieu* of using the personal data of data subjects to provide services to data subjects. The data controllers are expected to use eixisting capabilities, build new capabilities and process to meet the requirements of the reglation. There is always a dilemma when it comes to discuss between the rights of data subjects. It is important to protect the rights of data subjects, but laying down endless obligations on data controller is not always understood a balanced approach. As stated before, the principles mentioned under Art. 5 of the GDPR, create a bottleneck for processing data and to supplement it there are Rights of data subjects which the controller has to facilitate. The facilitation of these rights in itself creates practical obligation on data controllers which is not completely reflected through the black letter law.The controllers have to create process to facilitate the requests in relation to data subjets rights. To add to these obligations, Chapter 4 of the GDPR, lays down general obligations for data controllers. The accountability prinicple set out under Art. 5 is elborated and expanded under the provisons of chapter 4. The Chapter begins with abstract obligations not just to ensure that data privacy principles are met but also demonstrate the GDPR compliance. The essence of the chapter is to impose a procative role on data controller while processing personal data of data subjects, in order to provide services requested by them. The responsibility of demonstarting compliance creates another challenging series of work for the data controller to take up. It is generally the size of the organisation ad the nature of data being processed that determines the complexity of the process to demonstarte compliance. To sum up, there are huge gaps in understanding the reasons for processing personal data. The idea to restrict processing of personal data is understandble but the part that seems most under discussed is that the personal data is processed by data controller to provide services to data subjects, but the obligations and fines are only data controllers. The data subject availing the facilities/services can anytime revoke the use of those and exercise their rights. Another aspect of this duality is that rights acknowledged under chapter have twofold implications. It empowers the data subjects to

have better control of their personal data and also lays downs obligations on data controllers to create working processes to ensure that data subject's rights are facilitated. The work does not end here, by the virtue of art. 24, data controllers must not only comply with law but also demonstrate it creating further work for data controllers. There are many parameters to evalue this and it shall be done in subsequent chapters.

The rights of data subjects, and the direct obligation on data controllers to facilitate the rights under Chapter 3 of the GDPR, bring additional responsibilities arising from rights in Chapter 3 and direct obligations in Chapter 4 of the GDPR in the daily work life which is not evident from the regulation. The regulation expects the data controllers to create modalities to meet the requiremnts and requests from data subjects, but for small and medium organisations, having/developing the right tools, training employees, creating processes and modalities.

The current thesis is titled 'Balancing of rights of data subjects and data controllers under the GDPR' and aims to analyse the rights provided to data subjects and the obligations imposed on data controllers. This thesis intends to investigate the principles of the GDPR deeply, to come to an analysis-based conclusion on the issue. The purpose of the thesis is to evaluate the balancing of rights of data subjects and data controllers as stated in the provisions of the GDPR. The thesis will focus on the analysing the obligations on data controllers and rights of data subjects against the principles of proportionality, necessity and its effect on human rights of individuals. The thesis is an attempt to analyze the rights and obligations of individuals and data controllers under the General Data Protection Regulation (GDPR). This research aims at studying the principles of balancing of rights under the European Union (EU) and analyse those principles in relation to rights and obligation of data subjects and data controllers under the GDPR.

The GDPR under Chapter 3 *inter alia* acknowledges The Right to Access, Right to rectification, Right to Erasure, and Right to Object which shall be used as the basis to study the obligations on controllers when the data subjects exercise these rights and further analysed to see whether the rights and obligations of both the parties are balanced?

The thesis is twofold. One part of the thesis focuses upon understanding the concept of balancing of rights, its evolution and its elements within the EU legal regime while the other part focuses on rights and obligations of data controllers and data subjects.

The laws of the Union are balanced in essence. In cases like *Schmidberger v Austria*[12], *Viking* Line[13] *etc*. the theoretical aspect of balancing of rights has been thoroughly discussed by the Courts, however, not much has been argued about the balancing of rights of controller and data subjects in the courts.

This research brings out the opinion that the obligation on controllers is higher in all cases, and it is much more than meets the eyes. The idea behind having stringent obligations is acceptable to ensure protection of personal data of individuals but imposing humongous obligations on data controller can affect their ability to run the organisation, provide services to data subjects. It will also be in contradiction to the notion of balanced regulations in the European Union.

It is also important to understand that GDPR does not exist in isolation and a data controller while processing personal data, and ensuring fair, transparent, lawful use of personal data, also has to have measures, technical and organisational to ensure safety of personal data in applications, there is need for cyber security, data governance, controls environment *etc*.. The GDPR is part of the EU Digital Framework which comes into play in some or the other way casting further obligations on the data controller. Some of the supplementary regulations are listed below.

- Regulation on Free Flow of Non personal data (EU 2018/1807): The regulation aims towards free movement of non-personal data within EU. It introduces interoperability that indirectly affects controllers dealing with mixed data sets including personal and non-personal data.
- Data Governance Act: It seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data.[14] It aims to make more data available and facilitate data sharing across sectors and EU countries in order to leverage the potential of data for the benefit of European citizens and businesses.[15]

[12] Case C-112/00 *Schmidberger v Austria* [2003] ECR I-5659.
[13] Case C-438/05 *International Transport Workers' Federation and Finnish Seamen's Union v Viking Line* [2007] ECR I-10779
[14] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1
[15] Ibid

- Data Act: It emphasize fair access and user rights while protecting personal data and enhance the EU's data economy and foster a competitive data market.[16] It facilitates and promotes the exchange and use of data within the European Economic Area and harmonize rules on fair access to and use of data. Enable public sector access to private sector data for responding to public emergencies.[17]
- Digital Services Act and Digital markets Act: Introduces transparency and platform accountability that impacts data processing. Reinforce the ecosystem of trust and user empowerment in which GDPR foundational requirements.

In other words, the GDPR came into force in 2018, the digital landscape has evolved rapidly, prompting a shift from data protection to data sharing frameworks like the Data Governance Act (DGA) and the Data Act. The explosion of industrial and non-personal data created new opportunities for innovation, especially in AI and smart services, which GDPR alone couldn't address. There was growing recognition that secure and fair data sharing beyond personal data is essential for a competitive and data-driven EU economy. The DGA and Data Act aim to unlock data held by public bodies and private entities, ensuring trust, transparency, and interoperability in data exchanges. This marks a shift toward a balanced data ecosystem, where protection and sharing coexist to support both individual rights and collective progress.

At the outset, this research would like to specify that the current thesis will analyse the rights and obligations under the GDPR and the reference to any other legislation will only be peripheral. The thesis will not delve into other legislations which form part of the EU Digital framework. The thesis is aimed at understanding that the GDPR came into force to ensure protection of individual's right to protection of personal data. The Rights which paved the way for a separate law for protection of personal data were also individual centric. Data protection is considered as a modern and active right which carries checks to ensure that the right of an individual with respect to personal data is upheld. If the essence of the law is individual centric, can it be balanced? Through the explanations below the thesis intends to highlight the inclination of law towards protection of individuals. The thesis further intends to explain through cases that such rights are not absolute

[16] European Commission, 'Data Act | Shaping Europe's Digital Future' (Digital Strategy, 2023) <https://digital-strategy.ec.europa.eu/en/policies/data-act> accessed 12 April, 2025
[17] European Commission, 'Data Act | Shaping Europe's Digital Future' (Digital Strategy, 2023) <https://digital-strategy.ec.europa.eu/en/policies/data-act> accessed 12 April, 2025.

but must be restricted rarely and based on the explanation derive conclusions on balancing of rights and obligations.

1.2 Research Question

How is the balance between data subjects' rights and data controllers' obligations maintained in practice under the GDPR, and what challenges arise in its enforcement?

1.3 Structure of Chapters

1. Introduction

In this chapter, the thesis will cover the background and context of GDPR in the EU digital framework. This chapter will also lay the introduction for the need for balancing rights of data subjects and data controllers

2. Principles of Balancing Right

In this chapter of the thesis, the principle of proportionality, the principle of necessity and the importance of fundamental rights while bringing in any new regulation as elaborated upon. These principles are part of the general principles for the foundation of EU regulation, and the chapter covers this perspective.

3. Obligations of data controllers and rights of data subjects

In this chapter of the thesis a detailed obligations of data controller under multiples parts of the GDPR, especially chapter 3 and 4 has been discussed. This chapter focuses on the overlap of requirements for the data controller to meet through different provisions of the GDPR. The second part of the chapter covers the rights of data subjects such as access, rectification, objection, and erasure

4. Balancing Rights: Analysis

In this chapter of the thesis practical and legal analysis of how rights and obligations interact. The analysis is twofold, the fist part analyzes the presence of principles of proportionality, necessity and fundamental rights forming the essence of the GDPR and the second part discusses the operational challenges the data controller faces and the need to mitigate these.

5. Conclusion

In this chapter of the thesis, the synthesis of findings has been discussed and reflections on balance and recommendations

6. Bibliography

- References and sources

1.4 Purpose and Limitations

The purpose of the thesis is to analyze the balance between the rights of data subjects and the obligations of data controllers under the GDPR. The thesis aims to evaluate whether the GDPR achieves a fair balance using principles of proportionality, necessity, and fundamental rights and to use specific rights (access, rectification, objection, erasure) as lenses for analysis.

The limitations found by the research are many fold. This study is primarily theoretical, centering on the GDPR with only peripheral references to other EU digital regulations. Methodologically, it relies on doctrinal legal analysis, drawing from legislation, case law, and regulatory guidance, without incorporating empirical data or interviews. The empirical dimension is limited to documented cases and official reports, with no primary data collection. Analytically, the scope is confined to examining the provisions and practical implications of the GDPR. Ethically, the research respects confidentiality and legal boundaries, and does not involve accessing or processing personal data.

1.5 Mode of Research

This thesis majorly adopts a doctrinal methodology. This thesis involves a systematic analysis of legal texts, including legislation, case law, and academic commentary. The doctrinal research focuses on identifying, interpreting, and applying legal rules within a structured framework. In the present thesis, I applied this method by closely examining EU legal instruments such as the GDPR, Data Governance Act, and Data Act, analyzing their provisions, underlying principles, and interrelations to understand the evolving regulatory landscape around data protection and sharing. I have reviewed guidelines and official documents published by the European Data Protection Board (EDPB) and I have used comparative Case Study by examination of landmark cases (e.g., Google Spain, Digital Rights Ireland, Schrems II) to illustrate balancing in practice. I have conducted a critical analysis by evaluating how principles are operationalized and the practical

challenges faced by data controllers. The critical analysis is also influenced by the working knowledge of the legal principles I have acquired through my work.

II CHAPTER 2

The Principles of Proportionality, Necessity and Fundamental Rights as the tenets of EU law

Any legislation that comes into being within the EU, is governed by set of 'general principles'. The term 'general principles' indicate that these principles are not specific, rather it operates at a level of abstraction, but carries a weight to itself.[18] In the EU, the general principles are many folds and their categorisation depends on how the principle was derived.

The legal order of the EU is rooted not only in written treaties and secondary legislation but also in a body of general principles developed through the jurisprudence of the European Court of Justice (ECJ).[19] Among the most foundational are the principles of proportionality, necessity, and respect for fundamental rights, which operate as normative constraints on EU institutional power and serve as interpretative guides in legal adjudication.[20]

These general principles ensure that acts adopted by EU institutions are consistent with the overarching aims and values of the Union. The general principles are constitutionalized judicial doctrines that sit alongside treaty provisions as primary sources of EU law.[21] Proportionality, in particular, functions as a mechanism to ensure that public authorities do not exceed their mandates and that individual rights are not unjustifiably infringed.[22]

The ECJ has elevated proportionality into a universal principle of review, applying it across domains including digital regulation and privacy. Necessity is an embedded component of proportionality, it ensures that any restriction of rights or market freedoms is the least restrictive means of achieving a legitimate aim.[23] Fundamental rights, likewise, are treated not merely as policy considerations, but as structural norms grounded in the constitutional traditions common to the member states, ECHR, and the Charter of Fundamental Rights.[24]

[18] Takis Tridimas, *The General Principles of EU Law* (2nd edn, Oxford University Press 2006) 1
[19] Takis Tridimas, *The General Principles of EU Law* (2nd edn, Oxford University Press 2006) 1.
[20] Takis Tridimas, *The General Principles of EU Law* (2nd edn, Oxford University Press 2006) 1.
[21] Takis Tridimas, *The General Principles of EU Law* (2nd edn, Oxford University Press 2006) 1
[22] ibid 3–5
[23] Tor-Inge Harbo, *The Function of Proportionality Analysis in European Law* (Brill Nijhoff 2015) 23–24
[24] Takis Tridimas, *The General Principles of EU Law* (2nd edn, Oxford University Press 2006) 313-320

Together, these three principles: proportionality, necessity, and fundamental rights form an indivisible triad. Any attempt to legislate in their absence would not only undermine legal certainty but also threaten the legitimacy of the Union's constitutional framework.

2.1 The Principle of Proportionality

The principle of proportionality is a fundamental doctrine in EU law used to assess whether legal measures taken by the Union or its member states are legitimate and fair in light of the rights they affect. Originating from German public law and constitutional jurisprudence, it has since evolved into a general principle recognized across EU law. It requires that any limitation of rights or imposition of burdens by public authority be appropriately tailored to the legitimate objectives pursued.

The word proportionality in general means to do something in a balance[25]. The Principle of Proportionality was introduced with aim to strike a balance in the use of force necessary to get the results. It was by the Treaty of Maastricht in 1992, that the principle of proportionality was formally codified in EU law. It is worth noting that this was recognized by the Court of Justice of the EU much earlier. Its current iteration is in Article 5(4) of the Treaty on European Union (TEU), which provides that '*under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties'*.[26] The principle of proportionality in EU law was later developed in the Treaty on the Functioning of the European Union (TFEU), in particular in its Article 296(1), which expressly requires observing proportionality of the principle when EU legislative and administrative acts are adopted.[27] Proportionality is a principle found in a number of different areas of both international and domestic law, including the law of armed conflict, the law of treaties, the law regarding the use of force, maritime delimitation law, and human rights law. As such, it has a number of different permutations according to the specific area in which it operates.[28] The principle of proportionality

[25] New Balkans Office, *The Principle of Proportionality in Regulatory Matters in the Context of the EU Charter of Fundamental Rights* (EU, March 2025)
[26] New Balkans Office, *The Principle of Proportionality in Regulatory Matters in the Context of the EU Charter of Fundamental Rights* (EU, March 2025)
[27] New Balkans Office, *The Principle of Proportionality in Regulatory Matters in the Context of the EU Charter of Fundamental Rights* (EU, March 2025)
[28] Emily Crawford, 'Proportionality' (Oxford Public International Law, last updated May 2011) <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1446> accessed 27 April, 2025.

in EU law is neither expressed nor applied in the same way as the principle of proportionality under the European Convention on Human Rights.[29] Its scope widened in cases such as *R v Minister of Agriculture, ex p. Fedesa*, where the ECJ declared that a measure is disproportionate only if it is "manifestly inappropriate having regard to the objective pursued". Gradually, proportionality became a general principle of constitutional adjudication, capable of testing both EU and national measures.[30]

Proportionality as a general principle of European law, functions as a form of balancing for rights rather than binary legality.[31] EU jurisprudence often deploys the three tests of proportionality, necessity and alignment with Fundamental Rights without necessarily naming them. The application of these three principles are reflected implicitly in judgments concerning market freedoms, privacy, environmental law, and digital regulation. This tripartite structure ensures that proportionality necessity and alignment with FR operates both as a technical tool of judicial review and as a constitutional principle preserving the balance between competing values state authority and individual rights.[32]

The principle of proportionality contains, three subsets or three parameters namely suitability, necessity and *stricto sensu*. Proportionality is assessed based on the three tenets. In the subsequent paragraphs, this thesis will discuss more about it.

Suitability as a parameter of proportionality reflects upon suitability of a measure taken to achieve the result creating a relationship between the means applied and the result achieved. A measure is suitable to achieve its objective, i.e. it can achieve the said goal. purported objective.[33] The principle of suitability precludes the adoption of means that obstruct the realization of at least one principle without promoting any principle or goal for which it has been adopted.[34] When it comes

[29] Richmond Chambers, 'The Principle of Proportionality in EU Law – Part 1' (Richmond Chambers, 21 February 2022) <https://www.richmondchambers.com/news/the-principle-of-proportionality-in-eu-law-part-1/> accessed 27 April, 2025.
[30] Case C-331/88 *The Queen v Minister of Agriculture, Fisheries and Food, ex parte Fedesa* [1990] ECR I-4023
[31] Sieckmann (n 1) 117–120

[32] Richmond Chambers, 'The Principle of Proportionality in EU Law – Part 1' (Richmond Chambers, 21 February 2022) <https://www.richmondchambers.com/news/the-principle-of-proportionality-in-eu-law-part-1/> accessed 27 April, 2025
[33] New Balkans Office, *The Principle of Proportionality in Regulatory Matters in the Context of the EU Charter of Fundamental Rights* (EU, March 2025)
[34] Jan-R Sieckmann (ed), *Proportionality, Balancing, and Rights: Robert Alexy's Theory of Constitutional Rights* (Springer Nature Switzerland AG 2021) 2.

to regulations, it becomes outrightly irrational if a rule/law comes into force which is not suitable to meet the desired result. suitability test functions as a safety valve for erroneous administrative and legislative decision-making.[35] To assess suitability, the courts might also assess consistency in many cases. By adding the consistency test, the horizon of the suitability test is broadened. The broadening of the scope of the suitability test by way of requiring that the regulatory regime of a member state as a whole be consistent in light of the aim of the relevant legislative or administrative measure clearly implies that the threshold is set higher than where a narrower approach is taken.[36]

The next tenet of the principle of proportionality is necessity. It is the second step in assessing proportionality. In case, where a new legislation or measure is suitable, the next step is to see if it is necessary. The necessity test has been interpreted to mean that where there is a choice between several appropriate measures recourse must be had to the measure which restricts the infringed freedom the least.[37] Necessity as a tenet of proportionality leads to optimization of factual possibilities. Necessity requires evaluation and assessment of possible options and finding the one which is least intrusive. The sub-principle of necessity, has two steps to it, the first identifying the available options and the second is analyzing to decide the least intrusive one. For any rule, regulations or a law, it is not only important to be suitable but it is also important to have means and measures necessary to implement the requirement of the legislation and do not overarch the rights and freedoms of individuals.

The last tenet of the principle of proportionality is proportionality stricto sensu which means that the tenets of proportionality should be interpreted in the strictest/narrow way. In the case of *Fedesa and Others*[38]*, 'The Court stated that "the principle of proportionality requires that the prohibitory measures are appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to*

[35] *The Function of Proportionality Analysis in European Law*, Nijhoff Studies in EU Law, vol 8, eds Fabian Amtenbrink and Ramses A Wessel (Brill | Nijhoff 2021) 42.
[36] Jan-R Sieckmann (ed), *Proportionality, Balancing, and Rights: Robert Alexy's Theory of Constitutional Rights* (Springer Nature Switzerland AG 2021) 2., page 28
[37] *The Function of Proportionality Analysis in European Law*, Nijhoff Studies in EU Law, vol 8, eds Fabian Amtenbrink and Ramses A Wessel (Brill | Nijhoff 2021) 34.
[38] Case C-331/88 *The Queen v Minister of Agriculture, Fisheries and Food, ex parte Fedesa and others* [1990] ECR I-4023.

the aims pursued.' In other words the disadvantage caused by the measure should not be disproportionate to the advantages.[39] Proportionality stricto sensu is also referred as the balancing test wherein the benefits of the rights acknowledged and the level of interference on the rights are assessed. This principle requires a justification for limiting rights, rather constitutional rights. In other works the benefits arising from the right must outweigh the harm caused by infringement to the rights. Proportionality *stricto sensu* acts a balancing test to see if the measures used to achieve the intended objective is excessive or not.

After getting a broader understanding of the principle of proportionality, it is only natural to see its importance of the principle of proportionality in the GDPR. The GDPR is one of the most significant examples of proportionality's integration into EU secondary law. It reflects the need to balance individual rights to privacy and data protection with the legitimate interests of controllers, public authorities, and the functioning of the internal market. In the field of data privacy, where proportionality is concerned, it relates to adequate collection of data, data processed should be necessary and relevant to the purpose of processing. Proportionality is also seen in GDPR through data minimization, data retention and deletion, restriction of processing *et.al*..
The GDPR is a vital regulation that exemplifies the principle of proportionality by ensuring that data processing activities are balanced against the rights and freedoms of individuals. It requires that personal data be collected and processed only to the extent necessary for a specific purpose avoiding excessive intrusion. This balance is key to maintaining trust and fairness in the digital environment.

2.2 The Principle of Necessity

The concept of necessity operates as a foundational standard within EU constitutional and fundamental rights law, especially in the domain of personal data protection. As articulated in Article 52(1) of the Charter of Fundamental Rights, any limitation on a Charter, including those under Article 7 (privacy) and Article 8 (data protection), must meet several cumulative conditions, one of which is necessity. This principle ensures that fundamental rights are not unduly infringed by legislative or executive acts unless strictly justified.

[39] *The Function of Proportionality Analysis in European Law*, Nijhoff Studies in EU Law, vol 8, eds Fabian Amtenbrink and Ramses A Wessel (Brill | Nijhoff 2021) 36.

The significance of necessity is that it emerges not merely as a procedural hurdle but a substantive shield guarding against arbitrary and excessive intrusions into fundamental freedoms.

The necessity principle has evolved as a cross-pillar doctrine, bridging EU internal market law, human rights, and now increasingly, digital regulation. Its modern inception stems from CJEU interpretations of the Charter, particularly Articles 7 and 8, and has been shaped by decisions such as Digital Rights Ireland[40] and Schrems I[41] and II[42], which invalidated data retention and international data transfer frameworks, respectively, for failing necessity and proportionality assessments.[43] In the aforementioned cases, Digital Rights Ireland, Schrems I, and Schrems II, the Court of Justice of the European Union emphasized the principle of necessity as central to lawful data processing and surveillance. In Digital Rights Ireland, the Court invalidated the Data Retention Directive, holding that indiscriminate retention of communications data was not necessary for combating serious crime and violated fundamental rights. In *Schrems I*, the Court struck down the Safe Harbor framework, finding that U.S. surveillance practices lacked safeguards and exceeded what was necessary for national security. Similarly, in *Schrems II*, the Court invalidated the Privacy Shield, reaffirming that data transfers must be strictly necessary and proportionate, and that blanket surveillance without adequate protections breaches the necessity principle under EU law. These rulings collectively underscore that any interference with privacy must be justified by a legitimate aim and limited to what is strictly required.

The Necessity Toolkit published by the European Data Protection Supervisor (EDPS) represents a crystallisation of this doctrine into practical legislative assessment. It guides lawmakers on how to structure measures involving data processing so they withstand judicial scrutiny. The toolkit acknowledges that necessity is not an abstract or self-evident principle, but one that demands case-specific, factual, and evidence-based justification.[44]

---

[40] Case C-293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* [2014] ECLI:EU:C:2014:238

[41] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 (*Schrems I*)

[42] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* [2020] ECLI:EU:C:2020:559 (*Schrems II*)

[43] C-293/12 *Digital Rights Ireland Ltd v Minister for Communications* [2014] ECLI:EU:C:2014:238.

[44] European Data Protection Supervisor, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (11 April 2017) 2

The legal construction of the principle of Necessity under Article 52(1) CFR, states that any restriction on fundamental rights must:

1. Be provided for by law,
2. Respect the essence of the rights,
3. Serve a legitimate general interest or protect others' rights,
4. Be necessary, and
5. Be proportionate.

In essence, necessity demands that:

1. There is no less intrusive measure that could achieve the same legitimate aim;
2. The chosen measure is suitably customized and effective; and
3. The interference with rights is justified by clear, and justifiable reasoning.

The burden of proof lies on the legislator, not on the individual.[45] The measure must demonstrate why existing or less intrusive legal frameworks cannot adequately achieve the stated objective.

The EDPS Toolkit explains that necessity focuses on eliminating excessive or unjustified options, whereas proportionality considers whether the justified option is balanced and fair in its implementation.[46] Thus, necessity is often considered a component of proportionality, particularly in EU jurisprudence.

In the case of Tele2 Sverige[47], where the court invalidated a Swedish law mandating bulk data retention, holding that the measure was neither necessary nor proportionate, especially due to its lack of targeting and safeguards.[48] In this landmark judgement, the CJEU reinforced the principles of necessity and proportionality in EU data protection law. The Court held that general and indiscriminate retention of electronic communications data by service providers was incompatible with the Charter of Fundamental Rights. It emphasized that any data retention must be strictly necessary, targeted, and subject to robust safeguards such as judicial oversight. This judgment built

[45] European Data Protection Supervisor, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (11 April 2017) 6
[46] European Data Protection Supervisor, *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* (11 April 2017) 5-7
[47] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others* [2016] ECLI:EU:C:2016:970.
[48] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others* [2016] ECLI:EU:C:2016:970.

on earlier decisions like *Digital Rights Ireland*, affirming that privacy intrusions must be justified by a legitimate aim and proportionate to that aim core principles later echoed in the GDPR's framework for lawful data processing.

The CJEU, through multiple cases has emphasized the importance of necessity as an essential principle of European law. In the Digital Rights Ireland[49] (2014**),** the CJEU annulled the Data Retention Directive due to the blanket nature of data collection, which was not shown to be strictly necessary for crime prevention.[50]

- Schrems II (2020)[51]: The Court invalidated the EU-US Privacy Shield because US surveillance laws lacked necessity and proportionality safeguards for EU citizens.
- La Quadrature du Net (2020)[52]: Reaffirmed that only targeted retention is compatible with the Charter and that blanket surveillance fails the necessity threshold.

These cases emphasize that generalized data collection without specific justification will be struck down under necessity scrutiny.

The necessity principle acts as a legal checkpoint, preventing disproportionate infringements on fundamental rights. EU law has progressively adopted a strict necessity standard, particularly in data protection. The EDPS Toolkit provides a structured way to apply this principle in legislation, enhancing transparency, accountability, and fundamental rights compliance.

2.3 Fundamental Rights are the cornerstone of EU Law

The Fundamental Rights have emerged as a cornerstone of the EU legal order. This is reflected both in cases decided by CJEU and the codification of rights in the Charter. Fundamental rights

[49] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238.
[50] ibid
[51] C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II)* [2020] ECLI:EU:C:2020:559
[52] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791

function as guiding principles for the Union's legislative activities.Initially, the focus within the EU was on economic integration. The absence of explicit provisions on fundamental rights led to challenges regarding potential conflicts between EU law and domestic constitutional guarantees. The CJEU carefully case by case integrated fundamental rights as general principles of EU law.

In *Stauder v City of Ulm*[53], the Court recognised for the first time that fundamental rights formed part of the general principles protected by EU law. This was consolidated in *Internationale Handelsgesellschaft*,[54] where the Court emphasised that respect for fundamental rights was a condition of the validity of Community measures, even over national constitutions. In *Nold v Commission*[55], the Court grounded its rights jurisprudence in the constitutional traditions common to the member states and international instruments, notably the European Convention on human rights.

The Charter on FR provides the primary catalogue of rights binding on EU institutions and member states when implementing Union law. The Charter articulates a wide range of rights, but particularly relevant to the GDPR are: Article 7 (respect for private and family life), Article 8 (the explicit right to data protection), and Article 11 (freedom of expression and information, frequently balanced against privacy and data protection in digital contexts). The Charter functions both as a shield against EU overreach and a sword for individuals seeking to enforce their rights.[56] The GDPR's preamble reinforces this, declaring in Recital 1 that the regulation "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."

The CJEU has consistently acted as the primary guardian of fundamental rights, striking down EU legislation and international agreements incompatible with Charter rights. This role confirms that rights are not peripheral but foundational.

In *Digital Rights Ireland*[57] the Court invalidated the Data Retention Directive for disproportionate interference with Articles 7 and 8 of the Charter.The *Schrems* cases extended this approach to

[53] Case 29/69 *Stauder v City of Ulm* [1969] ECR 419
[54] Case 11/70 *Internationale Handelsgesellschaft* [1970] ECR 1125.
[55] Case 4/73 *Nold v Commission* [1974] ECR 491
[56] Koen Lenaerts, 'Exploring the limits of the EU Charter of Fundamental Rights' (2012) 8 *European Constitutional Law Review* 375.
[57] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238

international data transfers, invalidating first the Safe Harbor arrangement (Schrems I)[58] and later the EU–US Privacy Shield (Schrems II).[59] In both cases, the Court underscored the inadequacy of safeguards for EU citizens' rights under US surveillance practices.

The Court has also addressed balancing within the GDPR framework. In *Google Spain*[60], it recognised the "right to be forgotten", requiring search engines to delist results under certain conditions, thereby balancing data protection with freedom of expression. More recently, in *GC and Others*[61], the Court clarified the scope of erasure rights, again highlighting the need for proportional balancing.

Article 51 of the Charter obliges EU institutions to respect fundamental rights when creating new legislations. Fundamental rights have transformed from an absence in the founding Treaties to the cornerstone of EU law. Through CJEU case law, the codification of the Charter, and integration into legislative processes, rights now underpin both the validity and legitimacy of EU action. I other words, fundamental rights operate not only as legal constraints but as the normative foundation of EU law-making, ensuring that integration remains anchored in shared constitutional principles.

[58] Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650
[59] Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650
[60] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD)* [2014] ECLI:EU:C:2014:317.
[61] Case C-136/17 *GC and Others* [2019] ECLI:EU:C:2019:773

Chapter III

Obligations on data controllers and the rights of data subjects

The rights of data subjects under the GDPR do not exist in isolation. The rights acknowledged under Chapter III, provides data subjects with the power over their personal data and at the same time imposes obligations on data controllers. Chapter 4 of the GDPR lists down the obligations of data controllers in addition to the fundamental principles of data processing under art.5 GDPR, namely accountability, data minimization, accuracy, storage limitation and purpose limitation. Art. 5 of the GDPR, lists down the principles of fair processing and that also impose obligations on the data subjects. The rights guaranteed under Chapter 3 do place huge checks and obligation on controllers. The data controller has general obligations and specific obligations and the responsibility to facilitate the rights of data subjects. In the subsequent pages, this thesis will discuss the obligations of data controllers in first part and the rights of data subjects in the second part.

3.1 The Obligations on data controllers

In the subsequent paragraph we will see that the obligation on data controllers are intertwined throughout the GDPR. The direct obligations mentioned under chapter IV and Chapter V, also reflect the principles mentioned under Article 5 of the GDPR.

3.1.1 The obligations under chapter IV of the GDPR

The GDPR does not call for prohibiting the processing of persona data but it regulates the use of personal data. To ensure that personal data is processed in a safe and protected environment with requisite measures in place, the GDPR has laid down a list of measures which a data controller

must take to ensure that personal data is processed in a lawful manner. The GDPR lays down some specific requirements which the controller must meet and some general requirements. The specific requirements are triggered by general requirements sometimes.

Chapter IV of the GDPR, lays down the obligations of a data controller. Article 24 of the GDPR, places an general obligation on the data controller to do a generic risk assessment while processing data. When read with recitals 74, 75, 76, 77 and 78 it becomes clear that this general risk

assessment places an obligation on the data controller to demonstrate compliance with GDPR when processing personal data by implementing appropriate and effective measures. These measures can be organisational measures of technical measures. The controller also has to assess and evaluate risks to the rights of data subjects and it could include physical harm, material harm or non-material harm, like if the processing of data encroaches the right of data subject, what happens if there is breach of data, how to retrieve data etc.

In other words it can be said that this general obligation on controller which involves a blanket of risk assessments to be conducted, enforces the accountability principle under article 5(2) GDPR. This article assigns a proactive role to the controller, who has to ensure compliance with the GDPR at all stages of processing.[62] The obligation on the controller is not only to be compliant but also to demonstrate compliance under this Article. This could be understood by an example, Art. 24 GDPR, also emphasizes on implementing technical and organizational measures to secure personal data of data subjects, thus obliging the controller to demonstrate that he/she has taken measures to safeguard personal data.

On the same lines, the obligation to have appropriate technical and organizational measures is also imposed on the data controllers under article 32 of the GDPR. Article 25of the GDPR, puts an obligation on data controller to have Data Protection by design and default (DPbDD) in place. In simple words the concept of DPbDD puts an obligation on data controllers to maintain technical and organisational measures. This means that when programming, designing and conceptualizing systems and programs, as well as when acquiring systems and services from third parties, the controller has to ensure that data protection is taken into account and that the principles of the GDPR are properly integrated into the processing activity.[63]

Article 25 puts an accountability on the data controllers to meet the legal obligations for processing personal data. Under article 25(1) the controller shall implement appropriate technical and organizational measures which are designed to implement the data protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements and protect

[62]GDPRhub, 'Article 24 GDPR – Responsibility of the controller' (GDPRhub) <https://gdprhub.eu/Article_24_GDPR> accessed 10 June 2025.
[63]GDPRhub, 'Article 24 GDPR – Responsibility of the controller' (GDPRhub) <https://gdprhub.eu/Article_24_GDPR> accessed 10 June 2025.

the rights and freedoms of data subjects.[64] As per the EDPB guidelines on DPbDD appropriate measures and necessary safeguards are meant to serve the same purpose of protecting the rights of data subjects and ensuring that the protection of their personal data is built into the processing.[65] It is very clear that the extensive obligation put on the controller is aimed at protecting the rights of data subjects under the GDPR. Article 25 does not describe any specific measure but puts a responsibility on data controllers to design the technical measures to meet the processing requirements. This is also a general obligation on data controllers as under article24. Under article 24 as well as art. 25, the controller is obligated not only to have the measures in place but also responsible for demonstrating that the measures taken are effective.

The controller is obliged to maintain records of processing as per the requirements of Art. 30 if the GDPR. The data controller should maintain a record of processing activities under its responsibility. This will generally be a written document encompassing all the processing activities performed by a controller, regardless of whether the controller performs the processing itself or uses processors. In large organizations, who may have thousands of processes, it is extremely challenging and taxing to maintain elaborate records of processing. It is a must to have transparent and updated records of processing (ROP) because, that document reveals the process, the personal data involved in that processing, the lawful basis of processing, technical and organizational measures, has link to assessments conducted and applications storing data. An efficient ROP can support the controller when the data subject exercises his/her rights.

On one hand the ROP imposes the accountability requirement for data controllers by asking them create a track of processing activities and on other hand it improves the transparency of processing while increasing the transparency requirements for the data controller. In case of Right to access, the controller can trace the data and its uses, lawful basis assessment and purpose of processing. In case of erasure, it is easy to trace the applications where ethe data is and then subsequently either delete the data or archive the data in case of restriction to processing before erasure.

Art. 32 of the GDPR, obligates the data controller to have the have proper technical and organizational measures in place. The controller is also obligated to conduct an impact assessment

[64]European Data Protection Board, *Guidelines 4/2019 on Data Protection by Design and by Default*, Version 2.0, adopted on 20 October 2020, 6.
[65] European Data Protection Board, *Guidelines 4/2019 on Data Protection by Design and by Default*, Version 2.0, adopted on 20 October 2020,6.

on the processes. In order to meet the requirements of processing data in a lawful manner and to cater to the rights of data subjects, the data controller must have several risk assessments and measures in place.

As per art. 35, the data controller is obligated to conduct an Data Protection Impact Assessment (DPIA). Every processing operation that a data controller undertakes, needs to be impact assessed before it being processed. The data controller also needs to assess the inherent risks to rights of individuals while conducting the impact assessment.

3.1.2 Controllers obligation arising from lawfulness, fairness and transparency

The obligations imposed on data controller is to ensure that the personal data processing meets the requirement of fair, transparent and lawful processing. Through the obligations under Chapter IV, the controller is obligated to meet the requirements of transparency, fairness, lawful processing accountability, data minimization, purpose limitation , storage limitation, accuracy, integrity and confidentiality as provided in Art. 5.

Art. 5(1) refers to the principle of lawfulness, fairness and transparency. The GDPR does not define the word lawful, however for a processing to be lawful it must comply with the six lawful bases of processing under art. 6 of the GDPR. The six lawful bases are simple to follow but the real problem for data controllers begin in cases where personal data is being processed for outside the legal basis identified under the GDPR. This can include Anti Money Laundering laws, e-privacy directive, sanctions law etc. It is for those cases that the data controller needs to have an established and running legal support and capabilities to identify these additional processing requirements which exist outside the scope of art. 6 of the GDPR.

The principle of fairness mentioned under art. 5, has its roots in art. 8 of the Charter on Fundamental Rights and the accountability principle. The word fairness has not been defined in the GDPR and is often construed in the broadest possible way. It provides a general check on data controllers while processing personal data. The EDPB in the guidelines on Data Privacy by Design and default has provided an exhaustive list of fair processing. The list is particularly detailed and examples range from providing the data subject with a high level of autonomy in controlling the

processing, to the right to fair algorithms and human intervention.[66] Other important elements of fairness are officially recognized, such as the data subjects' expectation of reasonable use of their data, and the right not be discriminated or exploited as a consequence of certain psychological weaknesses.[67]

The Working Party (WP) defines it as "Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights".[68]

Transparency is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes.[69] It is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union.[70] The principle of transparency is closely linked to fairness and accountability under the GDPR. In other words, the data controller has an obligation, rather is accountable to demonstrate compliance with the GDPR principles[71] and when requested information can provide that information to data subject or authorities where it is legal necessity or mandate. The principle of transparency is an obligation for data controller but a tool of data subjects. It empowers the data subjects to hold the controller liable and accountable for processing of the personal data of data subjects outside the stated purposes. The concept of transparency in the GDPR is user-centric rather than legalistic and is realized by way of specific practical requirements on data controllers and processors through various provisions under the GDPR. See also the transparency guidelines by the Art 29 Working party.[72]

---

[66] GDPRhub, 'Article 5 GDPR – Principles relating to processing of personal data' (GDPRhub) <https://gdprhub.eu/Article_5_GDPR> accessed 10 June 2025.
[67] GDPRhub, 'Article 5 GDPR – Principles relating to processing of personal data' (GDPRhub) <https://gdprhub.eu/Article_5_GDPR> accessed 10 June 2025.
[68] Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679*, WP260 rev.01, adopted on 29 November 2017, revised and adopted on 11 April 2018, page 4.
[69] *ibid*
[70] *ibid*.
[71] Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679*, WP260 rev.01, adopted on 29 November 2017, revised and adopted on 11 April 2018, page 5.
[72] Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679*, WP260 rev.01, adopted on 29 November 2017, revised and adopted on 11 April 2018.

The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This is clear from Article 12 which provides that transparency applies at the following stages of the data processing cycle: [73]

- before or at the start of the data processing cycle, i.e. when the personal data is being collected either from the data subject or otherwise obtained;

- throughout the whole processing period, i.e. when communicating with data subjects about their rights; and

- at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing.

The principle of transparency, requires the data subject to be fully aware of how the data is being processed. The obligation of transparency can be seen in Art 12, Art. 13, Art. 15, Art. 24 where the data controller must record, Art . 30 and many more. Recital 39 of the GDPR contains a number of explanatory statements regarding the transparency principle. In particular, "*it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed"*. Data subjects should be "*made aware of risks, rules, safeguards, and rights in relation to the processing... and how to exercise their rights".*[74] All information communicated should be "*accessible and easy to understand*" and in "*clear and plain language*".[75] This principle establishes an obligation for the controller to take any appropriate measure in order to keep the data subjects who may be users, customers or clients informed about how their data are being used.[76] Transparency may refer to the information given to the individual before the processing starts, the

[73] Article 29 Data Protection Working Party *Guidelines on Transparency under Regulation* 2016/679, last revised and adopted on April11, 2018, page 6.
[74] GDPRhub, 'Article 5 GDPR – Principles relating to processing of personal data' (GDPRhub) <https://gdprhub.eu/Article_5_GDPR> accessed 27 March 2025.
[75] GDPRhub, 'Article 5 GDPR – Principles relating to processing of personal data' (GDPRhub) <https://gdprhub.eu/Article_5_GDPR> accessed 27 March 2025.
[76] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018 edn, Publications Office of the European Union 2018), page 120.

information that should be readily accessible to data subjects during the processing, but also to the information given to data subjects following a request of access to their own data.[77]

3.1.3 Obligations on Data Controllers arising from the principles of processing

In the second part of Art 5, the principles for processing are mentioned. These principles lay an obligation on data controllers in multiple ways. In the subsequent paragraphs we will look at the principles one by one.

3.1.3.1 Purpose Limitation

In case of purpose limitation, any personal data that is being processed should be processed for a pre-defined purpose, if the processing exceeds the purpose for which the data was originally collected for, then the processing in incompliant with the provision of Art. 5 (1) (b) GDPR. The principle of purpose limitation is closely related with the principle of transparency. The controller, in case he processes data for purpose other than what he/she collected the data for, in such cases the data controller must conduct a purpose compatibility assessment (PCA) (mentioned in guidelines provided by the Finnish DPA on DPIA[78]). In the PCA, the controller assess, if the data subject has reasonable expectation, the nature of data, data categories are same and the same lawful basis is valid for the new purpose, in such cases, the controller can process the data for the new purpose. The purpose limitation also keeps the data controllers in check for not processing the personal data for an entirely new purpose without informing the data subject and being non-compliant with the principle of transparency and fairness. It is important to note here that the Finnish DPA in its guidelines has provided sample questions for PCA which the data subject can take inspiration from. However, the burden of moulding the questions to meet the organisational needs, set up a process to do this and bring in capabilities to manage the process.

3.1.3.2 Data minimization

In the case of data minimization, the controller is obligated to process only that data which is a must for processing activity. This is closely related with the principle of accountability, and fairness. Only such data shall be processed as are “adequate, relevant and not excessive in relation

[77] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018 edn, Publications Office of the European Union 2018), page 120.
[78] Office of the Data Protection Ombudsman (Finland), *Guidelines for Data Protection Impact Assessment (DPIA)*, 2021 <https://tietosuoja.fi/en/data-protection-impact-assessment> accessed 27 October 2025.

to the purpose for which they are collected and/or further processed.[79] The data controller is obliged to restrict collection of data to what is strictly necessary. The controller also has an obligation to inform the data subject about the nature and purpose of processing, at the time of data collection.

3.1.3.3 Accuracy

The principle of accuracy, makes the data controller obligated to keep accurate data on data subject. This is very closely related to the right to rectification under Art. 15. The principle of accuracy comes with its limitation, at times to document the chronology of event, the data cannot be rectified to make accurate and in some other cases, rectifying and making data accurate is considered as the most urgent. The principle of accuracy also meddles with right to erasure. This can be understood with a simple example: In a case where A takes loan form the bank and has B be his surety for the loan. After the loan has been repaid, the data needs to be stored for a long time as per local law regulations. In this case, the data of surety can also be stored for accuracy purposes.

3.1.3.4 Storage limitation

As per storage limitation principle the controller must delete the personal data of data subject after the purpose for processing that data is over. This is directly linked to the retention of data. Lawful storage of data which are no longer needed could, therefore, be achieved by anonymizing data. Retention of data is tracked by local legislation, other requirements like Anti Money laundering, sanctions, labor laws, insurance laws, pension laws, employment regulations. The controller is responsible for keeping the personal data in retention mode for a specific time and not indefinitely. The data controller must create a repository to store this state, have technical measures, firewalls, info sec measures, cyber security measures to keep the data safe from external attacks. The controller not only needs to create but also trains employees in organizational measures, so that no employee processes the data while it is in retention mode. Creating a technical solution requires multiple capabilities including IT, legal, privacy, information security etc. Once that solution is created it needs to be impact assessed as a new product because it will retain data which is processing of personal data. Meaning a tool used for processing personal data, forms part of processing operations, thus needs to be impact assessed as per Art. 35. Each data may be affected

[79] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018 edn, Publications Office of the European Union 2018), page 122

by different local laws and the controller must have capabilities to keep the particular data in alignment with legal requirements. The controller is also responsible for deleting the data after the retention period comes to an end.

3.1.3.5 Integrity and confidentiality

The principle of integrity and confidentiality under the GDPR requires that personal data be processed in a manner that ensures appropriate security. This includes protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Data controllers and processors must implement suitable technical and organizational measures such as encryption, access controls, and regular security assessments to safeguard personal data. The goal is to maintain the trust of data subjects and uphold their rights by preventing data breaches and ensuring that only authorized individuals can access or handle personal information**.** This puts a huge obligation data controllers not only to establish processes to protect data but also establish process to report breaches internally and also to the local DPA where required by law.

3.1.3.6 Accountability

Under the GDPR places a legal obligation on data controllers to not only comply with the regulation's requirements but also to be able to demonstrate that compliance[80]. This means organizations must actively implement measures such as data protection policies, staff training, documentation of processing activities, and regular audits to ensure adherence to GDPR principles. Accountability emphasizes proactive responsibility that controllers must show that they have considered data protection in all aspects of processing and can provide evidence of their efforts. It reinforces transparency and trust, ensuring that data subjects' rights are respected and safeguarded throughout the data lifecycle.

Thus, the obligation on data controller, not only comes from Chapter IV, but we see it is laid down in Art. 5 as well. The principles of Art. 5 are closely linked to the rights provided to data subjects under chapter III. In other words, the obligation on data controllers not only from the oligations listed for them to follow but also from the rights f data subjects acknowledged under chapter III. The Art. 5 principles which cast a generic obligation are found to play a role in multiple provisions

[80] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 24

of the GDPR and are a emphasized through those. What skips the academic eye, is the operational work the facilitation of the rights and aforementioned obligations demand. The cost is an important aspect but the continuous efforts to create the process, developing capabilities, training employees, managing data subjects requests, having separate processes to deal with vulnerable data subjects is even more. The controller has to constantly thrive to ensure that there is privacy compliance and the requirements of the legislation are met.

3.2 Rights of Data Subjects under the GDPR

Chapter III of the GDPR acknowledges the rights of data subjects. In the subsequent paragraphs we will be briefly touch on the Right to Access, and discuss Right to rectification, Right to Object and Right to Erasure.

3.2.1 Right to Access

Right to Access as acknowledged by the GDPR, has its roots in Article 8 of the European Charter on Fundamental Rights. This right is now elaborated under art. 15 of the GDPR. The aim of Right to Access is to provide individuals with access to information on how an organisation or controllers are processing personal data and allow the data subjects to have control over the processing of their own personal data. The right of access is thus designed to enable natural persons to have control over personal data relating to them in that it allows them, "to be aware of, and verify, the lawfulness of the processing.[81] It is a tool for the individuals to know how an organisation is processing data, on what basis is the data being processed, the lawfulness of the processing, the accuracy of the same despite the technological developments. In other words, it is aimed at providing simple, clear and lucid information to the data subjects. The EDPP has also stated that the controller should only focus on what is that the data subjected has requested to access and not on why has he/she exercised the right to access.[82] It is not for the controller to decide whether the request for access should be entertained or not but the controller must only be concerned with

[81] European Data Protection Board, *Guidelines 01/2022 on Rights of Data Subjects: Right of Access*, Version 2.0, adopted on 28 March 2023, 10.
[82] European Data Protection Board, *Guidelines 01/2022 on the Right of Access*, Version 2.0, adopted on 28 March 2023

meeting the right to access request as per the legislative guidance, meaning, the controller must provide the information in a machine readable format, within 30 days.

The EDPB states that the modalities of the right of access are now specified more precisely in the GDPR, this right is also more instructive from the point of legal certainty for both the data subject and the controller. Besides, the specific wording of Art. 15, and the precise deadline for the provision of data under Art. 12(3) GDPR, obliges the controller to be prepared for data subject inquiries by developing procedures for handling requests.[83]

Right to access must not be read in isolation as it also gives way to right to rectification, objection to processing, and right to erasure. Meaning, if a data subject knows how their data is being processed and what personal data is being processed by the organisation, they can request for right to erasure, restriction of processing of right to rectification. It is pertinent to note that the other Rights guaranteed to data subject under Chapter 3 of the GDPR are not dependent on the Right to Access.

The scope of right to access under the GDPR extends to all personal data, activity logs and also pseudonymized data. The Right to access is not an absolute right is carefully balanced. It is available for only one's own personal data and does not extend to someone else's personal data. Organisation and controllers must not overly interpret this right. In cases where data of several person are categorised or saved in a similar format or together, then the controller must be careful while adhering to the rights of Access of the data subject. In such cases the controller cannot provide all the information, including information on other persons, it would amount to breach of data. The controller must isolate the data of the person exercising right to access and then give information.

The European Data Protection Board (EDPB) in their guidelines have discussed the structure of Right to access The elements of Art. 15(1) and (2) together define the content of the right of access, art.15(3) deals with the modalities of access, in addition to the general requirements set out in art. 12 GDPR and art. 15(4) supplements the limits and restrictions that art. 12(5) GDPR provides for

[83] European Data Protection Board, *Guidelines 01/2022 on Rights of Data Subjects: Right of Access*, Version 2.0, adopted on 28 March 2023, 9.

all data subjects' rights with a specific focus on rights and freedoms of others in the context of access.[84]

The right of access includes three different components under art 15(1) and (2):[85]

1. Confirmation as to whether data about the person is processed or not,
2. Access to this personal data and
3. Access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers.

The next paragraphs will elaborate upon the components.

Confirmation as to weather personal data is processed or not

This is the first step in the request to Right to Access. At the outset, the data subject needs to know whether the controller is processing data or not. If the controller is not processing data then the question regarding how, why, activity logs do not arise. If the controller does not process the data subject's personal data then he/she just has to inform that to the data subject and close the request.

However, if the data is in retention mode and is not accessible to any employee, the controller must inform that to the data subject. When data is in retention mode, it is not being processed by the controller as there is no lawful basis for processing the data but due to requirements found in other law example, MIFID, Anti money laundering law, anti terrorism laws, sanctions etc., the data needs to be stored for a certain period of time before being deleted.

To sum up, if the controller is not processing data subject's personal data, then he/she just needs to inform that to the data subject and no further question arises except for in cases where the controller has the personal data of the data subject in retention mode, in such cases if the data subject requests information on retention of his/her data, the controller is obliged to give that information. When in retention mode the data is not being processed by the controller but the controller in essence still has access to the data subject's personal data. If the controller processes

[84] European Data Protection Board, *Guidelines 01/2022 on Rights of Data Subjects: Right of Access*, Version 2.0, adopted on 28 March 2023, 12

[85] European Data Protection Board, *Guidelines 01/2022 on Rights of Data Subjects: Right of Access*, Version 2.0, adopted on 28 March 2023, 12.

data subject's personal data while it is in retention mode, the data subject can bring a suit for breach of personal data and violation of rights under the GDPR of the data subject. In that case the controller would have not used the data is a fair and transparent manner which is also acknowledged under the right to access.

Access to personal data being processed

This is the next component under the Right to Access and pivotal to the Right to Access. The Right to Access is aimed at providing information regarding the processing of data to the data subjects. Aside from basic personal data like name and address, an unlimited variety of data may fall within this definition, provided that they fall under the material scope of the GDPR, notably with regards to the way in which there are processed.[86] Under the right to access, a data subject has right to receive a detailed and elaborate explanation meaning not only categories of data or a general description but a detailed one. Article 15 of the GDPR acknowledges the Right to access of the data which is directly collected as per article 13 and 14 of the GDPR refers to an obligation on data controllers with the operative word being 'provide'[87] The obligation is to the controller to provide information to the data subject. The controller must make the information available in a way that the data subject gets a clear understanding and detailed picture but there also lies an inherent obligation on the controller to simplify the complex information so that an average data subject can understand. This obligation also results in a contradiction, at one place the GDPR wants the information to be concise, clear and sufficient. It is practically impossible for controllers to process data for multiple purposes and large scale. The WP in its guidelines states that the modality on providing information can be decided by the controller, but such modality does not exonerate a data controller from meeting the GDPR guidelines and recommendations while providing information.[88]

In the Spotify case[89], (Sweden), the music giant has been fine 5 million euros. The complaint argued the music streaming platform failed to provide all personal data requested; did not provide

[86] European Data Protection Board, *Guidelines 01/2022 on Rights of Data Subjects: Right of Access*, Version 2.0, adopted on 28 March 2023, Page 12
[87] European Data Protection Board, *Guidelines 01/2022 on Rights of Data Subjects: Right of Access*, Version 2.0, adopted on 28 March 2023, Page 18
[88] European Data Protection Board, *Guidelines 01/2022 on the Right of Access*, Version 2.0, adopted on 28 March 2023
[89] Swedish Authority for Privacy Protection (IMY), *Decision against Spotify AB regarding the right of access under the GDPR*, Decision No. DI-2020-4061, 13 June 2023

information on the purposes of the processing; nor on recipients; and also did not provide information on international transfers, among other allegations.[90] Thus, the obligation on data controller to be fair, transparent and provide detailed information about processing of data is high.

This might not be as simple for the data controllers. In large organizations were data is stored across multiple systems and huge amount of data is being processed, it is difficult for data controllers to provide all information and yet keep it concise.

For data controllers, any request made by the data subject is treated as referring to all personal data. If the data controller provides only a selection of personal data then the risk is that the data subject might assume that to be complete information and later this can lead to breach of guidelines under the GDPR. The problem on the part of the controller is two-fold, the risk of providing less information and developing internal capabilities to be able to provide details on all personal data being processed even in most complex forms of processing.

In such cases, the controller can decide on providing information to the data subject in a layered manner. Meaning, the vast information can be categorized in different groups or layers and the granular information about each group and be in different layers. In a real world it is challenging for regular data subjects to understand how to deal with information in groups or understand why the information is in groups. The data controller would have an additional duty to inform the data subjects about the grouping approach. The data controller must have that information available before the right to access is submitted. Giving information in group or layered format does not mean that the controller can refrain from providing all information. It is only a way to provide vast information in such format that it is easily understandable for the data subject and more structured to maintain internally for data controllers.

The GDPR has not talked about the layered approach but the art. 20 WP in its document on transparency[91] has discussed layered approach for controllers while providing information to data subject. The WP has not defined the term layered approach but has discussed it in the digital context and volume of information that the data controller needs to provide data subject. The layered approach is a way to maintain transparency about processing of data by the data controller,

[90] Spotify fined in Sweden over GDPR data access complaint | TechCrunch, last visited on June 30, 2025.
[91] Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679*, WP260 rev.01, adopted on 29 November 2017

but it is not a collection of multiple privacy notice. Layered approach is about providing the most sensitive or important information first and the same information can be elaborated further in different layers along with less sensitive information. The WP recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue.[92] Layered privacy statements/ notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read.[93] The data controller is free to choose to structure of the layers but must be vigilant that the layers do not contain contradicting information. The WP29 in its recommendations has stated that Layer 1 should contain information on purpose of processing, identity of the data controller and a description of data subject's rights.[94] The recommendation of the WP29 is in light of the principle of fairness, and owing to that in Layer 1, the controller must provide information that affects the data subject most and i.e lawful basis of processing. The concept of layered approach has mostly been discussed in digital environment, but it is possible to use the layered approach even in non-digital formats. The Working Party 29 reflects that in non-digital context, information can be provided over phone call, in person meetings etc. through hard copy/paper environments.

The Information Commissioner's Office, UK, which is an adequate country from the GDPR's perspective has also elaborated upon the definition of layered approach. It is an approach where the data controller share information on processing of personal data to data subject in layers, meaning the key information can be in layer 1, such as lawful basis of processing, basic information etc.[95] The second and third layer can have further information on processing of personal data. The first layer is generally crisp and short but the second and the third layers have more elaborate and detailed information. The discretion is on the data controller regarding which data the controller wants to keep in layer 1, layer 2 or layer 3. Providing information in layered

[92] Article 29 Data Protection Working Party Guidelines on Transparency under Regulation 2016/679, last revised and adopted on April11, 2018, page 19
[93] Article 29 Data Protection Working Party Guidelines on Transparency under Regulation 2016/679, last revised and adopted on April11, 2018, page 19
[94] Article 29 Data Protection Working Party Guidelines on Transparency under Regulation 2016/679, last revised and adopted on April11, 2018, page 19
[95] Information Commissioner's Office, 'What methods can we use to provide privacy information?' (ICO) <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/what-methods-can-we-use-to-provide-privacy-information/> accessed 10 March 2023.

form is not synonymous to providing less information. It does not dispense the data controller from the obligation of transparency and fairness. As stated above, the layered approach makes it easier for controller to keep records in structured format and provide information quickly when the controller is processing large quantity of personal data under different lawful basis of processing. Layered approach is best suited when information is provided in online format as the links provided as easy to access when in online format.

To sum up it can be said that access to personal data is an integral part of Right to Access, and the data controller is obliged to provide all information related to data subject on processing. It is however, on the data controller to decide the means and ways to provide information, but despite the modalities and form of providing information, the information should be complete. The use of internet access is very high in Europe and most parts of the world, and for companies having a digital presence, layered approach can be one of the most efficient ways to do it. As explained above, it is one of the modes that has been suggested by Working party 29 and ICO in UK.

Access to information about processing

Proving information about processing of personal data is another component of Right to Access. As per article 15(1) and 15(2) of the GDPR, the obligation is on data controller to provide the information on processing to data subject to data subject. Article 30 of the GDPR puts an obligation on the controller to maintain a records of processing of each personal data of every data subject and while providing the information on processing, the controller can use the records of processing it has created. The interlinkage of article 15 and 30 can be understood in 2 steps.

A. The GDPR puts an obligation on data controller and data processor to maintain a records of processing under the GDPR. This Records of processing of contains a wide of information as directed by the GDPR. Article 30, Paragraph 1 specifies the information that the controller must include in the record. Paragraph 2 serves the same purpose, but it is addressed to the processor, Paragraph 3 clarifies that the record must be in written form, possibly also in electronic form, paragraph 4, states that the record must be provided to supervisory authorities when they request it. Finally, the last paragraph establishes exceptions to the obligation to keep the record for controllers.[96]

[96] GDPRhub, 'Article 30 GDPR – Records of processing activities' (GDPRhub) <https://gdprhub.eu/Article_30_GDPR> accessed 20 March 2024.

B. The same records which the controller is obligated to maintain under art. 30 can be used by the data controller while providing information to the data subjects. If the data controller decides to use Layered approach parts of this information can be included in layer 1.

While providing the information the data controller must be transparent and not hide any information about processing of personal data of the data subject. The obligation on data controller is also to provide up to date information. While providing information the data controller must provide precise information with regards to processing activities on data. If there multiple basis of processing personal data then the data controller must identify and clarify that which category of data is being processed under which legal basis and also the purposes of processing. Unlike Art. 13(1)(c) and Art. 14(1)(c) GDPR, the information on the processing referred to in Art. 15(1)(a) does not contain information on the legal basis for the processing. However, as some data subjects' rights depend on the applicable legal basis, this information is important for the data subjects to verify the lawfulness of the data processing and to determine which data subject's rights are applicable in the specific situation.[97] Therefore, in order to facilitate the exercise of data subjects' rights in line with Art. 12(2) GDPR, the controller is recommended to also inform the data subject as to the applicable legal basis for each processing operation or to indicate where they can find this information.[98] In certain situations, the controller must all need to tailor these information as per the need and requirements of data subject.

Thus, the obligation is on the data controller to ensure that the data subject gets the information in an precise yet elaborate manner.

These were the element of Right to Access but what does it really mean for the data controller in the practical sense. The expenditure to meet the obligations is much more and many times the most appropriate measures are not appropriate in eyes of the court/law.

[97] European Data Protection Board, *Guidelines 01/2022 on Rights of Data Subjects: Right of Access*, Version 2.0, adopted on 28 March 2023, 38.
[98] European Data Protection Board, *Guidelines 01/2022 on Rights of Data Subjects: Right of Access*, Version 2.0, adopted on 28 March 2023, 38.

In a large organization where personal data is processed heavily and is spread across different systems and applications, the data controller at the inception needs to establish an access process. The establishment of process is challenging, complex and financially extensive.

At the outset the controller needs to establish a mechanism to have the data in one place, or if the data is in several applications then there needs to be a capability that helps in pulling all that data together before it is provided to the data subject. The capability needs to be technically advanced and connected to all applications and components within applications to be able to pull all the information on a data subject together, within a specific time. The work of data controller does not stop here. In cases where vast quantity of information is involved due to large scale of processing activities carried out on the personal data, the controller can use layered approach to provide the information to the data subject. Meaning, after the controller has managed to gather all information regarding the processing at one place, it needs to be in a proper format, in simple language so that the data subject can understand even the most technical and complex details. In case of complex details, it becomes rather challenging for data controllers to simplify the information without skipping the details. The other challenge faced by data controllers in such cases is that many times employees handling such requests are unable to understand the very nature or format of information requested by data subject. For example: In an organization, a data subject requested some information in machine readable format, like. CSV,. JSON etc. but the person handling the request did not understand the meaning of machine-readable format and how to process that request. The data subject was provided with the information he needed after a lot of effort and investment by the data controller. Multiple resources from technical teams were involved and a lot of manual work went in. Now in such cases, the problem is two-fold, the lack of knowledge of the person handling that request and the amount of time spent on converting the information into what was requested by the data subject.

The resources at the data controllers end is not limited to create a process or developing technical and non-technical capabilities but regularly training employees, ensuring that employees involved in assessing Right to Access are well aware of the GDPR guidelines and have access to means in case of complex requests.

3.2.2 Right to Rectification

Article 16 of the GDPR acknowledges right to rectification. The right to rectification allows a data subject to ask the Data Controller to rectify any inaccuracies in personal data the controller has on the data subject. Inaccurate data includes incomplete data, so data subjects can also request that the controller completes any partial data, which might be achieved by providing the controller with a supplementary statement. The processing of incorrect or incomplete data can lead to possibly severe disadvantages for the data subject increasing the risk of exclusion, discrimination, or defamation.[99] The Right to rectification has two parts to it;

i. the first is the right to rectify incorrect information and
ii. the second is the right to complete incomplete information.

The notion is to avoid misrepresentation or inaccurate representation which can lead to biases against the data subject. The Right to rectification comes into force only when the data subject exercises his/her rights and reaches out to the controller. After the data subject has exercised his/her rights the accountability is on the data controller to ensure that inaccurate data is either erase, rectified or amended.[100] The controller is obligated to responds to the request of Right to rectification within one month of receiving the request or in some cases within 2 months. The controller must verify the identity of data subject before addressing the right of rectification. In case of legally significant matters the controller can ask data subject to provide a proof of inaccuracy.[101] Despite having the onus to prove the data subject cannot be refused from exercising this right (exceptions applicable). If the controller has shared information regarding the data subject to a processor, then the obligation is on a controller to ensure that the inaccuracies are rectified at the processor's end.

The right to rectification is also explicitly named as a fundamental right in Article 8(2) CFR. It is therefore important that it is interpreted in the light of the Charter and the principle of proportionality in Article 52(1) CFR.[102] The Right to rectification finds its root in the Principle of Accuracy under the GDPR. Article 5 (1)(d) of the GDPR requires the controller to keep the data

[99] GDPRhub, 'Article 16 GDPR – Right to rectification' (GDPRhub)
[100] Eduardo Ustaran (ed), *European Data Protection: Law and Practice* (2nd edn, IAPP 2019) 153.
[101] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018 edn, Publications Office of the European Union 2018) 220.
[102] GDPRhub, 'Article 16 GDPR – Right to rectification' (GDPRhub)

accurate and up to date wherever required. The GDPR, however hasn't described the term 'accurate'. Besides being good practice for any business, this protects the data subject from a number of threats, such as identity theft. [103] Controllers are required to make sure that personal data is accurate and, when needed, maintained up to date. They also have to take all reasonable measures to guarantee that erroneous personal data is promptly deleted or corrected, taking into account the purposes for which it is processed. Controllers should, in particular, accurately record the information they receive or gather, along with the information's original source.

The Right to Rectification is also imposed upon the data controller through the implementation the principle of accuracy under the Art. 5(1)(d) of the GDPR. The controller is obligated to take every necessary step to ensure that data is rectified and is accurate. It is important to have accurate data not just to avoid biases but also to ensure that where needed, inaccurate information should not cause health related or life-threatening risks to data subject. Incorrect data can lead to multiple drawbacks. Here are some examples:[104]

- Denied services: Incorrect address details might prevent you from receiving deliveries or accessing services.
- Missed opportunities: Outdated contact information could lead to missed job offers or important communications.
- Discrimination: Inaccurate data used for profiling or automated decision-making could result in unfair treatment.
- Identity theft: Incorrect information can make you more vulnerable to fraud and identity theft

The question of rectification is also dependent on the industry and usage of data by the data controller. The controller should maintain the information current if it plans to use it for anything that depends on it staying current. For instance, whenever there is a pay increase, you should update your employee payroll data.[105] In a similar vein, you should update your data if a consumer moves so that the right place receives the items. In cases where updating personal data would be counterproductive to the intended use, then it is not required. For instance, updating the data could

[103] IT Governance Privacy Team, *EU GDPR: An Implementation and Compliance Guide* (4th edn, IT Governance Publishing 2020) 54.
[104] Principle Defence, 'Your GDPR Rights Explained – The Right to Rectification' <https://principledefence.com/your-gdpr-rights-explained-the-right-to-rectification/> accessed 27 January 2024.
[105] Information Commissioner's Office, 'The Principle of Accuracy' (ICO) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/> accessed 27 January 2024.

be counterproductive if you solely retain personal information for statistical, historical, or other research purposes.

At the operational end, meeting right to rectification can generate substantial amount of work for a controller, and a controller must meet the requirements within the span of a month. In case of a large organization the controller can provide the information within two months.

As stated above, the right to rectification has two parts to it. The right to rectify incorrect data and the right to complete. The GDPR does not define the inaccurate data but the right to rectify inaccurate data can be used to rectify facts. The Right to rectification can be used to rectify only facts and information even when such error is not by mistake but done purposefully. It is not possible to rectify opinion or value judgements under the right to rectification. Mere value judgements cannot be "inaccurate", predictions, forecasts and objective facts can be inaccurate but it may be even feasible to rectify the value judgment *itself*, when the underlying facts and/or the decision-making process are objectively wrong.[106] In the case of Peter Nowak[107] the CJEU highlighted that in cases where the examiner has made comments in regards an evaluation of answers but if the student number is wrongly written or the first page of the examination sheet which has records of identifying students is tied to another sheet, then in such cases, the comments by the examiner which is a value judgement is inaccurate as it is not for the student who wrote the answer.

Article 16 also provides the right to complete data, but the determination of 'incomplete' is proportional and dependent upon the purpose of processing personal data. The right to complete personal data can be done through supplementary statements.

The implementation of Right to Rectification poses significant work at the end data controller. The problem can be many folds for the data controller to access this right. At first, the extent to Right to Rectification can be quite diverse. It can be in form of simple typos and outdated information and also extend beyond the menial errors. The Right to rectification can include situations where the data held about an individual is misleading or gives a false impression. For instance, if your purchase history with an online retailer is inaccurate, leading to targeted advertising that does not

[106] GDPRhub, 'Article 16 GDPR – Right to rectification' (GDPRhub)
[107] C-434/16 *Peter Nowak v. Data Protection Commissioner*, ECLI:EU:C:2017:994

align with your interests, you can invoke your right to rectification to have this corrected. The right to rectification covers a range of information including.[108]

- Identifying information: Your name, address, contact details, online identifiers, etc.
- Descriptive data: Age, gender, nationality, occupation, etc.
- Financial information: Bank account details, credit card information, etc.
- Health data: Medical records, diagnoses, treatments, etc.
- Online activity: Browsing history, purchase history, social media activity, etc.

Any information that identifies or can be used to identify you falls under the scope of the right to rectification.

The other problem is when a right to rectification is requested, it can give rise to additional requirements while requesting rectification. At times, the request for rectification, can cause additional problems of maintaining accuracy for data controller to keep the data accurate. For example, in case of loan applications where surety is appointed while taking load or information on collateral assets is collected by the financial institution, the controller might want to delete some data therein but the controller cannot delete the data as deleting some aspects of the information can make the data incomplete, hence inaccurate. In such cases, the controller is obliged to maintain data accuracy. In another case where a couple took mortgage together and later, they separate and one spouse is in witness protection, it becomes and additional problem for the financial institute to keep the data accurate but also ensure that data of the spouse under witness protection like the new address/changed identity of spouse, is also update to keep the data accurate. The financial institution also has to ensure that such data is not visible to the other spouse. The amount of work to facilitate the right to rectification is enormous on data controller but the process that is set up to facilitate that right is another continuous work by the data controller.

The pre work must be done by the organisations to ensure that when a request for Right to Rectification is received, the controller has the means to meet the requirements. At the outset is establishing a data management system. Data controllers need to set up procedures that allow them to quickly find, confirm, and correct erroneous data. This necessitates a solid data management system that can adapt to changes without compromising the accuracy and integrity of the entire

[108] Principle Defence, 'Your GDPR Rights Explained – The Right to Rectification' <https://principledefence.com/your-gdpr-rights-explained-the-right-to-rectification/> accessed 27 January 2024.

dataset. Building such efficient and huge data management system requires immense monetary expense at the controllers' end. Thus, it requires proper resource allocation by the data controllers. The controller must allocate resource for technical developments, employee trainings to ensure such requests are handle in the right manner. The data controller must also account for cases where there is substantial right to rectification received, this would also depend on the industry and the purpose of processing. If the employer requires current data, then the cost of regular rectification may rise.

Establishing a process to deal with the request is next most important step., and the data controller must have the data mapped for rectification and maintain the full process to meet the requirements. This entails creating interfaces that are easy to use so that data subjects may submit requests, setting up channels of communication that are specifically dedicated for this purpose, and making sure that the personnel who handle these requests are properly trained. Having complicated process is likely to prove detrimental.

The communication channels set up must be easy to follow. The individuals applying for right to rectification must get clear guidelines about approaching and filing a request, clear information on status of the application and at which step the application is. Individuals must be informed about any delays, and outcome of the request for rectification. Not having a proper communication channel and failing to respond and updating status of the request will cause reputational damage to the organisation and weaken the consumer's trust.

One of the most important parts of receiving request for rectification of data is verifying customers. The data controllers must have adequate processes in place and robust verification mechanisms to verify the identity of the requester and the genuineness of the request for rectification.

The data controller must also be prepared for auditing trails, proper records and processes must be maintained to compliance and also be prepared in cases of audit.

The impact of receiving a request for rectification would vary from one data controller to another depending on the size of the organization, the kind of data being processed and the places where data is stored in an organisation. An important observation here is that many data subjects fill in incorrect information on online sites, to be able to use the services of the website. The data subject

has the freedom to upload inaccurate information but the obligation is on data controllers to maintain accurate data.

3.2.3 Right to Object

Article 21 of GDPR guarantees the Right to object. A key aspect of the GDPR that promotes personal autonomy is the "Right to Object." Under certain conditions, this right gives data subjects the power to object to and limit the processing of their personal information. Data subjects can invoke their right to object to personal data processing on grounds relating to their particular situation and to data processed for direct marketing purposes.[109] The Right to Object can be used in cases where the processing of their personal data for direct marketing, processing is carried out under legitimate interest or for historical and scientific purposes as specified under Art. 6(1)(e) and (f) of the GDPR. The right to Object can also be brought in force in cases of profiling. "Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information."[110]

The right to object on grounds relating to the data subjects' particular situation aims to strike the correct balance between the data subject's data protection rights and the legitimate rights of others in processing their data.[111] The first part of the article gives data subjects a general right to object when data is processes as per Art. 6(1) and section 2 and 3 of the Art. give an unrestricted right to object in case of profiling and direct marketing. Art. 21(4) also lays an obligation on data controllers to inform the data subjects about their right to object.

The right to object requires discussion on several fronts:

---

[109] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018 edn, Publications Office of the European Union 2018) 229.
[110] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, recital 79.
[111] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018 edn, Publications Office of the European Union 2018) 230.

1. In accordance with processing (Art. 6(1)(e), (f))
2. In cases of Profiling
3. Digital Marketing

Right to Object in case of Legitimate Interest Art. 6(1) (e) and (f)

Art. 21gives a general objection right to data subjects in case data is processed in accordance with Art 6(1) (e) and (f). In this case, the right of data subject is not absolute, but in cases where a data subject raises an objection, the data controller will have to prove a compelling legitimate grounds for processing data processing activity which overrides the data subject's interests, rights, and freedoms, or for the establishment, exercise, or defense of claims. If the data subject, uses the right to object and supplements is with appropriate justification.[112] The use of the words '*on grounds relating to his or her particular situation'* gives data subject a wide scope in this case of general objection to processing of personal data, meaning the particular situation can depend on the social, legal, economic or any other personal situation of the data subject. It is possible that the controller was not aware of this situation when the processing started or this situation did not exist when the processing of personal data began. However, on the other hand, the data subject cannot merely request the right to object, it must be supported by appropriate justification.

As stated in the GDPR hub, a Frankfurt Regional Court, which deemed a plaintiff's difficulties in looking for an apartment due to the disclosure of data about his debt to be sufficient.[113] The phrase "*relating to his or her particular situation*" simply indicates that the data subject should have the right to affirm their specific interests in their personal data not being processed, which the controller may consider (or reconsider, in the light of the data subject's individual position) in its weighing of interests.[114]

The EDPB states that a controller should not dismiss an objection by a data subject just because they did not elaborate much on their particular situation in their objection under Article 21(1) GDPR, rather the controller should ask data subject to specify the justifications.[115] The GDPR does not specify the extent to which objection can be made to processing of personal data but further

[112] GDPRhub, 'Article 21 GDPR – Right to object' (GDPRhub).
[113] LG Frankfurt am Main, 20 December 2018, referenced in GDPRhub, 'Article 21 GDPR – Right to object' (GDPRhub) <https://gdprhub.eu/index.php?title=Article_21_GDPR#(1)_Right_to_object> accessed 27 June 2025.
[114] GDPRhub, 'Article 21 GDPR – Right to object' (GDPRhub)
[115] GDPRhub, 'Article 21 GDPR – Right to object' (GDPRhub)

reading of the section highlights cases of direct marketing and profiling which does points towards the fact that, different forms of processing or purpose of processing is also within the scope.

Art. 6(1) (e) describes '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' Consequently, the right to object applies to cases where the controller has initially considered the prevalence of their defended interest, specifically, the public interest in the case of Article 6(1)(e) and the controller's legitimate interest in the case of Article 6(1)(f). In other words, there is a balancing of interests carried out by the controller at the core of the processing.[116] And if the data subject, uses his Right to Object with appropriate justification, the controller will have to prove that With respect to Art. 6(1) (f) which refers to use of legitimate interest as a basis of processing personal data, the GDPR does not define the term 'legitimate interest' but it puts an obligation on the data controller to weight the legitimate interest against the fundamental rights of the data subjects. Under the GDPR, the controller has the right to process data under legitimate interest. However, it is after the outcome of balancing test, that applicability of Legitimate interest as basis of processing can be decided.[117] For the other modes of processing it is assumed that the rights are balanced and only the test of necessity if required but in case of processing based on legitimate interest, a separate balancing test is needed which acts as an additional safeguard against inappropriate use of personal data by data controllers.[118] Thus, for processing of personal data on the grounds of legitimate interest would require the test of necessity and the balancing test.

There are two parts to balancing test:[119]

a. Identifying and analysing the legitimate interest claim
b. Evaluating Fundamental Rights.

<u>Legitimate Interest</u>

[116] GDPRhub, 'Article 21 GDPR – Right to object' (GDPRhub)
[117] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP217, adopted in April 2014, 9.
[118] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP217, adopted in April 2014, 10.
[119] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP217, adopted on 9 April 2014.

The concept of a legitimate interest can encompass a wide range of interests, from unimportant to highly compelling, simple to contentious. Article 29 Working party (WP) in its evaluation on legitimate interest has defined a difference between interest and purpose. The precise reason why the data are processed the goal or intention of the data processing is referred to as the "purpose" in the context of data protection. Conversely, an interest refers to a controller's larger investment in the processing or the gain that the controller gets from the processing, or that society could get from the processing. In order to conduct a balancing test against the interests and fundamental rights of the data subject, an interest must be sufficiently clearly expressed. Furthermore, the stakeholder's interest needs to be "pursued by the controller." This necessitates a genuine and immediate interest in anything that aligns with ongoing operations or benefits anticipated in the near future of the processing. Interest should be certain and not vague. It should be lawful, and can be practised in accordance with the GDPR.

To summarise legitimate interest' must therefore:[120]

- be lawful (i.e. in accordance with applicable EU and national law);
- be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific);
- represent a real and present interest (i.e. not be speculative).

Article 6(f) not only covers the legitimate interest of controllers but also of third parties. Thus, after having understood the essence of legitimate interest for data controllers, it is the need to also evaluate the legitimate interest of third parties.

In this case, the right to process personal data is not automatically revoked but one should understand that it being a general restriction, the controller will stop the processing after the assessment of balancing rights. It is an obligation on data controller to immediately begin the assessment after the request to objection of processing of personal data is received. If the request is attested with proper justification, then the controller needs to prove that his interests is compelling enough to override the rights of data subjects or the processing is necessary for establishment, exercise or defense of legal claims. The requirement of the section also puts an obligation on data controllers to immediately halt processing and delete data, however deletion of

[120] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217 page 25(April 2014).

data is traced back from other legislations and the controller is obliged to create a process to gather the requirements on deletion and if deletion is not permitted by law but objection to processing is valid, then the data controller needs to create another process, develop capabilities to ensure that this request from data subject is met in one form or another. The burden of proving whether the processing is due to compelling needs is also on the data controller. The GDPR does not define the word 'compelling'. WP29 suggested in its 'Guidelines on Automated Individual Decision-Making' that processing may be based on a compelling legitimate ground where, instead of merely furthering the controller's business interests, it is beneficial for society at large.

Right to Object in case of Digital Marketing

The word 'direct marketing is not defined in the GDPR, however the meaning can be inferred and derived from other legislations., like the E-privacy directive[121], unfair commercial practises directive[122], Digital Services Act[123]. For marketing to be direct, it is necessary an underlying activity by which the user is singled out and addressed with promoting materials concerning the sale of goods or the provision of services.[124] Article 13 of Directive 2002/58/EC (e-Privacy Directive, consolidated version) states that this scenario includes the use of automated calling machines, telefaxes, and e-mails, including SMS messages. The extent to which targeted advertising may be classified as direct marketing is not entirely clear, there is room for a broad interpretation of such a provision. Sophisticated online targeted advertising techniques do single-out and specifically target individual users across the internet to promote goods or services, and in this way appear to satisfy direct marketing's key characteristics.

Art. 21 (2) of the GDPR gives absolute right to the data subject to object to processing of personal data

1. in case of direct marketing and

[121] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.
[122] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) [2005] OJ L149/22.
[123] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
[124] GDPRhub, 'Article 21 GDPR – Right to object' (GDPRhub) <https://gdprhub.eu/Article_21_GDPR> accessed 20 April, 2025.

2. In case of profiling to the extent it is used for direct marketing.

When a data subject applies the right to object to direct marketing, the controller is obligated to stop the processing immediately. The request only affects the processing of personal data for direct marketing or profiling used in case of direct marketing. If the controller is processing data under any other lawful basis, then the controller is not obligated to halt the processing. The Right to object in such cases is closely linked to the right to erasure under Art. 17 of the GDPR. Art. 17(c) directs the data controller to delete the data of data subjects in case where the data subject has applied for right to object and there is no legitimate interest or any compelling ground for the data controller to keep the data. This also applies in cases of direct marketing.

As per Art. 21 (2) '*Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing**, which includes profiling to the extent that it is related to such direct marketing**.'* The GDPR defines profiling under Art. 4(4) as, 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements'. The GDPR is not focused on the results that come out as a matter of profiling but the processing of personal data carried out using profiling.

As per the definition given by the GDPR, profiling has 3 elements:

i. Some form of automated processing
ii. Processing of personal data
iii. Used for evaluation, analysis and to predict personal aspects about a natural person

In case of profiling there must be some form of automated processing, the definition *prima facie* does not specify about interference of human involvement and such processing is done for evaluation of personal data. A simple classification of individuals based on known characteristics such as their age, sex, and height does not necessarily lead to profiling.[125] This will depend on the purpose of the classification. In case of profiling, the data subjects are unaware of the process or

[125] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251 rev.01, adopted on 3 October 2017, revised and adopted on 6 February 2018, page 7.

the algorithm used to profile personal data. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves.[126] When a profiling is done for direct marketing, the data subject has an absolute right to request the controller to stop the processing of personal data then and there and by the virtue of art. 17(c), the data subject can request, deletion of such data. In other words, when a data subject exercises his/her right under art 21(2) then it means that there is no need for any balancing of interests; the controller must respect the individual's wishes without questioning the reasons for the objection. Recital 70 provides additional context to this right and says that it may be exercised at any time and free of charge.[127]

After evaluating the right of data subject acknowledged under Art 21, it is important to understand its effects and the obligation, it imposes on the data controllers. According to the GDPR, a data controller must inform the data subjects about the Right to Object at the time collecting personal data. The data controller must provide the data subjects with a clear and easily accessible information on how to exercise the rights. At the outset there isn't a standard format to apply for Right to Object. A data subject and can send a mail to the data controller requesting to stop processing his/her personal data. At this point, the controller is obligated to respond without delay and within 30 days. In practice, the work on data controllers is even more, specially if it an old and big organization. The controller, after he/she receives the request will have to ascertain all the areas and applications where the data of a data subject is stored. The data in many cases can be stored in cloud technology. After this mapping, if the right is exercised under 21(2), the data controller will utilize the legal expertise to understand in whether the Right to Erasure applicable under art. 17(c) is legally possible or not. If erasure of such data is not allowed due to implications from other local laws, *etc*. then the controller will have to stop the processing but store the data, which will cost money to the controller. The controller will also have to develop capabilities around technical measures to ensure that data in retention period safe.

---

[126] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251 rev.01, adopted on 3 October 2017, revised and adopted on 6 February 2018 ,page 9.

[127] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251 rev.01, adopted on 3 October 2017, revised and adopted on 6 February 2018, 19

If the request is made under Art. 21(1), then the controller is obliged to used Risk managers in the organization to map assess the appropriate justification made by the data subject and conduct an assessment for compelling interests by the controller. Leaving data out of data sets can often disrupt the processing purpose. To maintain accurate data is also an obligation on data controller, and the right to object does not specify to what extent a data subject can object to processing of that. This can cause issues with accuracy of data if some data is deleted and the algorithm or the process has issues due to inaccuracy.

In the One-Stop Thematic case object, has assessed the cases scenarios linked with Right to Object. The documents highlights three particular elements relevant to the exercise of the right to object:[128]

i. the information provided to the data subject about the right to object,
ii. the solutions – including technical solutions – adopted to make the exercise of this right easier, and,
iii. the implementation of appropriate procedures to handle such requests

In the Norwegian case of the Komplett bank[129], the bank customers were getting direct marketing messages and emails without any information on how to exercise the right to object or the information on opt out. This was opposed to the requirements under art. 13 in general and art. 13(2) (b) in specific and the data controller had faltered in upkeeping his/her obligations under the GDPR. This case is also relevant in highlighting some recurring shortcomings in the technical and organizational solutions adopted by controllers in dealing with this type of request. These include lack of capacity and backlogs in customer service departments as well as incorrect processing of objection requests where the data subject's request was not properly registered resulting in the implementation of the objection with regard to only one account in a case of multiple user accounts and technical errors within the system creating delays in complying with art. 21.[130] Through this case we see the extended obligations on data controller. The controller is obliged to facilitate the right of data subject, the right which is exercised under art. 21 and is related to objection to processing. The interesting part is that the obligations under art 5

[128] Alessandro Mantelero, 'One-Stop-Shop Thematic Case Digest – Right to Object' (GDPRhub, 9 December 2022) 5 a<https://gdprhub.eu/Thematic_Case_Digest:_Right_to_Object> accessed 20 April 2025.
[129] Datatilsynet (Norwegian Data Protection Authority), 'Decision against Komplett Bank ASA – Right to Object' (GDPRhub) <https://gdprhub.eu/index.php?title=Datatilsynet_-_Komplett_Bank_ASA> accessed 22 April, 2025.
[130] Alessandro Mantelero, 'One-Stop-Shop Thematic Case Digest – Right to Object' (GDPRhub, 9 December 2022) 2 <https://gdprhub.eu/Thematic_Case_Digest:_Right_to_Object> accessed 20 April 2025.

(transparency, fairness, lawfulness), art. 12 (transparent information), art. 13 and art. 14 (providing information to data subjects) are also applicable. The obligation to be compliant with art. 24 (general obligation on data controller to have the requisites and document compliance), art. 25 (by having proper technical and organizational measures should also be in place. If the data controller is unable to meet these requirements, there can be situations where the data privacy compliance at controller's end shall be questioned and assessed.

The case digest has also highlighted that most data controllers had less advanced internal process to deal with Right to object request. The interna process has deficiencies relating to handling of process, time frame needed, internal communication and lack of procedural structure to deal with the request lifecycle. The obligation is on data controller to establish a simple process and develop internal controls to check the efficiency of the process. In other words, it is on data controllers to establish specific procedures to process objection requests including appropriate technical solutions. It must therefore be adopted by data controllers, involving data processors according to the task distribution relating to processing operations, being aware that an incorrect task allocation may delay an appropriate response. In addition, the technical solutions implemented must be effective and designed with the different types of data subject in mind.[131]

To sum up the observations, in case of right to object, we can see that there is balancing at the level of using the right, meaning, the under art. 21(1), the data subject has to provide appropriate justification and if the controller can prove compelling interest then he/she can still process personal data. However, the larger burden is on the data controller in order to facilitate the rights. The data controller has the burden to establish a process, communicate the process to data subjects, ensure the necessary information is provided, and then maintain the process to meet the compliance guidelines, the actual facilitation of the right is a whole different story.

3.2.3 RIGHT TO ERASURE

Art. 17 of the GDPR elaborates upon the Right to Erasure, also known as the Right to be Forgotten. Article 17 (1) sets out a general principle to erase the data in the six following cases:

[131] Alessandro Mantelero, 'One-Stop-Shop Thematic Case Digest – Right to Object' (GDPRhub, 9 December 2022) 4 <https://gdprhub.eu/Thematic_Case_Digest:_Right_to_Object> accessed 27 April 2025.

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
2. the data subject withdraws consent on which the processing is based
3. the data subject exercised his or her Right to object to processing of his or her personal data pursuant to art. 21.1 and 21.2 GDPR
4. the personal data have been unlawfully processed
5. the erasure is compliant with a legal obligation
6. personal data has been collected in relation to the offer of information society services to a minor.

The Right to Erasure was first acknowledged by the CJEU in the case of *Google Spain and Google*[132] as an aspect of the right to privacy of data subjects related to processing of personal data by internet search engines in the context of delisting requests. The CJEU interpreted the relevant data protection framework in force at that time, in the light of the fundamental rights under articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union (hereinafter "the Charter").[133] The notion of Right to Erasure is multifaceted and has been construed in multiple ways. It initially surfaced as a component o data subject's rights to privacy in context of processing personal data in a CJEU ruling. The CJEU emphasized the basic rights guaranteed by the EU Charter of Fundamental Rights. Subsequently a new aspect of the right emerged, rising above the print material. The new aspect was in context of digitization, as the chances of information resurface was higher in case of digitally available data.

The Right to Erasure is not an absolute right and is dependent on local laws. Art. 17 in paragraph 1 establishes a standard "*right to deletion*" of personal data and imposes an obligation on the controller to remove the data when certain conditions are met. To enhance the effectiveness of the right to deletion, especially on the internet (Recital 66), paragraph 2 introduces the so-called "*right to be forgotten*" which imposes a further obligation on the controller to inform other recipients of the request to delete all links, copies or duplicates of the data, through appropriate technical and

[132] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, [2014] OJ C 212/4.
[133] European Court of Human Rights and Court of Justice of the European Union, *Joint Fact Sheet – Right to be Forgotten: ECtHR and CJEU Case-Law*, last updated 28 February 2025, 2

cost-effective measures.[134] Paragraph 3 sets out the exceptions to the rules outlined in paragraphs 1 and 2, which highlight the existing grounds for the legal processing of personal data in various parts of the GDPR.

The GDPR does not specify the time for keeping or deleting the records by the data controllers except in case of bookkeeping, where the controller can keep data for 6 years. The GDPR provides for a right to obtain from the controller the erasure of an individual's personal data without undue delay, when those data are no longer necessary in relation to the purposes for which they were collected or processed, following withdrawal of the consent on which data processing was originally based, or when the data had been processed unlawfully.[135] The Right to Erasure, is closely linked to data minimization, and storage limitation the controller should not process data that is no longer required.

The discourse of Right to Erasure is interesting to go through in the light of how this right unfolded for data subjects and with that how the obligations changed, rather multiplied for data controllers. The facilitation of right to Erasure became more complex as it expanded from deletion and removal of data from documents to delisting from search engines and social media pages. In the subsequent paragraphs we will through case see the expansion of the right to erasure and then look into delisting from search engines and social media pages.

Balancing of interest on individual requesting the erasure and others

In cases of right to erasure, it has to weighed whether the right of individual requesting deletion overweighs the right of others to have the information. In the case of Salvatore Manni[136], the CJEU was called upon to determine if EU law recognized a right to obtain erasure of personal data

[134] GDPRhub, 'Article 17 GDPR – Right to erasure ("right to be forgotten")' (GDPRhub) <https://gdprhub.eu/Article_17_GDPR> accessed 10 May, 2025.
[135] European Court of Human Rights and Court of Justice of the European Union, *Joint Factsheet – Right to be Forgotten: ECtHR and CJEU Case-Law* (last updated 28 February 2025) page 2.
[136] Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* ECLI:EU:C:2017:197.

from a Chamber of Commerce register, on the basis that that information prejudiced his potential clients and could have a negative impact on his commercial interests. In reaching its conclusion, the CJEU balanced EU data protection rules and Mr. Manni's commercial interest in removing the information about his former company's bankruptcy with the public interest in access to the information. It took due note of the fact that disclosure to the public registry of companies was provided for by law. The disclosure was important to protect the interests of third parties who may want to conduct business with a specific company. In view of the importance of the legitimate aim pursued by the register, the CJEU held that Mr. Manni did not have a right to obtain erasure of his personal data, as the need to protect the interests of third parties in relation to joint-stock and limited liability companies, and to ensure legal certainty, fair trading and thus the proper functioning of the internal market, took precedence over his rights under data protection legislation. However, the CJEU held that it could not be excluded that there may be specific situations in which the overriding and legitimate reasons relating to the specific case of the person concerned justify exceptionally that access to personal data entered in the register is limited, upon the expiry of a sufficiently long period to third parties who can demonstrate a specific interest in their consultation.

Prohibition to Publish and Removal of Information

In the case of , *Mediengruppe Österreich GmbH v. Austria*[137] the applicant requested prohibition of publication of picture and data on his brother who was referred as neo-Nazi. The court held that publication of crime which he had previously committed can be published and does not violate the right to privacy but ordered on not publishing the picture as it could prove detrimental to his right to private life. The Court ensured that balance was maintained.

In the case of *Węgrzynowski and Smolczewski* v. *Poland*,[138] two lawyers complained that a newspaper article that was damaging to their reputation continued to be accessible to the public on the newspaper's website. The lawyers requested the removal of the article, which alleged that they had made a fortune by assisting politicians in dubious business deals. The domestic courts, ruling on an earlier defamation action, had held that the article in question was based on insufficient

[137] *Mediengruppe Österreich GmbH v Austria*, App no 37713/18 (ECtHR, 28 April 2022)
[138] *Węgrzynowski and Smolczewski v Poland*, App no 33846/07 (ECtHR, 16 July 2013).

information and was in breach of the rights of the persons concerned.[139] The ECtHR noted that, it was not the role of judicial authorities to remove from the public domain all traces of publications which had in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations. It further emphasized that the applicant did not seek to secure the effective protection of his reputation by less restrictive means than total removal. The ECtHR concluded that the domestic courts' refusal to remove the article was not disproportionate.[140]

Alteration of information

The case concerned the refusal of the German Federal Court of Justice to prohibit three different media organizations from keeping on their respective Internet portals press files concerning the applicants' conviction for the murder of a well-known actor, in which the applicants were referred to by their full names. In assessing whether a fair balance had been struck between the applicants' rights under article 8 and the media organizations' freedom of expression and the public's freedom of information under article 10.[141] The court stated that the fact that at the time the applicants' requests for anonymization were lodged the impugned reports had continued to contribute to a debate of public interest; the fact that the applicants were not simply private individuals unknown to the public; the applicants' conduct with regard to the media, which they had approached after their conviction with a view to having the proceedings reopened; the fact that the reports had related the facts in an objective manner and without the intention to present the applicants in a disparaging way or to harm their reputation; and the limited accessibility of the information.[142]

From the above cases, it is clearly visible that the EtCHR has maintained a balance between right of data subjects who have requested for erasure and the rights of other individuals who have a valid right to receive information. The right extends from removal of information to prohibition to publish. A data controller is responsible to ensure that such information is deleted, removed form the places where he published.

---

[139] European Court of Human Rights and Court of Justice of the European Union, *Joint Factsheet – Right to be Forgotten: ECtHR and CJEU Case-Law* (last updated 28 February 2025) 5.
[140] European Court of Human Rights and Court of Justice of the European Union, *Joint Factsheet – Right to be Forgotten: ECtHR and CJEU Case-Law* (last updated 28 February 2025) page 11.
[141] European Court of Human Rights and Court of Justice of the European Union, *Joint Factsheet – Right to be Forgotten: ECtHR and CJEU Case-Law* (last updated 28 February 2025) page 11.
[142] European Court of Human Rights and Court of Justice of the European Union, *Joint Factsheet – Right to be Forgotten: ECtHR and CJEU Case-Law* (last updated 28 February 2025) page 11.

In the next part, we will discuss about the Right to Erasure in case of search engines and digital platforms. In cases of delisting, the main criteria is that the search should not be available by the name of the data subject but it can be available by any other search criteria. The word delisting has not been defined in the GDPR. Delisting requests do not result in the personal data being completely erased, instead the personal data will neither be erased from the source website nor from the index and cache of the search engine provider.[143]

As per art. 17(1) of the GDPR, a data subject can request a search engine provider, following a search carried out as a general rule on the basis of his or her name, to delist content from its search results, where the data subject's personal data returned in those search results are no longer necessary in relation to the purposes of the processing by the search engine.[144] This provision allows the data subject to request for removal of his/her data from the search engines in cases where their data is has an online presence for a longer time. For example, in many cases even after an employee has left the organization, their details like pictures, phone number is still kept on the employe's website. As the employee has left the organization, their records don't need to be public.

As per art. 17(1) (b), a data subject may request data controller for erasure i.e deleting their data as an effect of withdrawal of consent for processing personal data. In such cases, the publisher of information will have to notify the search engine to delist the information of the data subject. In the Google 2[145] judgement, the court has held that:[146]

'*The Court indicates that "(…) the consent must be 'specific' and must therefore relate specifically to the processing carried out in connection with the activity of the search engine (…). In practice, it is scarcely conceivable (…) that the operator of a search engine will seek the express consent of data subjects before processing personal data concerning them for the purposes of his referencing activity. In any event, (…) the mere fact that a person makes a request for de-referencing means,*

[143] European Data Protection Board, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in search engines cases under the GDPR (Part 1)*, Version 2.0, adopted on 12 July 2019, page 5.
[144] European Data Protection Board, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in search engines cases under the GDPR (Part 1)*, Version 2.0, adopted on 12 July 2019, page 7.
[145] Case C-136/17 *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:773, [2019] OJ C 424/8.
[146] European Data Protection Board, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in search engines cases under the GDPR (Part 1)*, Version 2.0, adopted on 12 July 2019, page 8

in principle, at least at the time of making the request, that he or she no longer consents to the processing carried out by the operator of the search engine.'

In such cases, it is on data controller to justify that consent was the only was and there was no less intrusive way to process personal data. The controller will also have to develop process to connect with search engines to ensure such delisting happens. The costs on small business operating websites is too high. The establishing of process is a cumbersome process and constantly training employees to ensure such request is met within time.

Request for Erasure of data in case of art. 17 (c) has been discussed in the section above on Right to Object. In subsequent section the data subject can request for erasure when the data is being processed unlawfully (art. 17 (1)(d)) and in cases where data is needs to be deleted as per legal requirements (art. 17 (1)(e)). In case of legal requirements, its not just the GDPR but several other laws like the Law Enforcement Directorate, Labor Laws, Banking laws etc. It is an obligation on data controllers to collect requirements from other laws to ensure that legal requirements are met.

With the development in technology, the cases requesting right to erasure have mainly been related to; erasure of data where it used for marketing purposes, unsolicited emails and for deletion of accounts, since the data subject is not using it anymore. This is true for the digital cases meaning where the data is available for online platforms *etc*., but in cases of banking industries, finance industries, legal departments, healthcare, such deletion does not come easy and in many cases, it is not even possible for data controllers to easily delete the information.

In case of right to erasure, the question for controllers is not only about erasing data but also retaining data, as required by or traced back from other legislations. The controller is obligated t establish an internal process to receive the right to erasure, a second internal process to collect all the information that is scattered through different applications within the organization, a third process to reach out to legal departments and find if there is any law that prohibits deletion of data at that point, a fourth process to check GDPR requirements of accuracy, meaning if deleting data makes rest of the record inaccurate. The data controller has to ensure that all of this is done within a time frame of thirty days. An additional procedure that data controllers have to do through if the data cannot be deleted is to retain the data and archive it, so that processing of the same is halted. For retaining data, there is specific retention period based on purpose of processing data. The data controller has to create a retention process, has to invest in tools to create a repository for retaining

the data based on data subject's request and then ensure that it is deleted after the purpose of retention is met. An additional requirement for data controller is that the when a repository or a technical solution for such retention is created, a Data Protection Impact Assessment (DPIA) under art. 35 of the GDPR has to be conducted, the process of retention needs to be impact assessed as art. 35 calls for processing operation to be impact assessed. This also needs to be documented as per the requirement under art. 24 of the GDPR. By virtue of art. 35 of the GDPR, there should be proper technical and organizational measures in place to facilitate the right to erasure, b.) If the right cannot be facilitated then, measures to keep the data safe in retention mode.

The obligations on data controllers are all in all quite huge and run throughout the GDPR. In this chapter we saw the rights, the obligation on data controllers to facilitate the rights, the obligations on data controllers laid down under art. 5, Chapter IV of the GDPR. Chapter V of the GDPR under art. 24, the Controller not just needs to facilitate the rights but also documents the process. Even though, the whole of chapter IV obligates the data controllers to maintain Records of Processing, conduct DPIA on processing operations, record the outcome, Conduct a general assessment of inherent risks under art. 24 of the GDPR. If the data is transferred outside EU/EEA, then the controller has to conduct a Transfer Impact Assessment (TIA) which requires evaluating the regulations in other countries (if they are not adequate countries). In the aforementioned arguments, we did see that the EDPB or judicial system through cases have tried to create a balance between the rights of data subjects requesting access, erasure, objection to processing, rectification and the right of others to have that information. Such balancing was seen mostly in cases of right to erasure cases where the court balanced the right of data subject requesting erasure with right of others to have information. The rights acknowledged under chapter III are not absolute in nature but do impose obligation of facilitation and creation of internal processes to meet the facilitation on data controllers. The facilitation and the internal processes are guided by the GDPR but governed by controls environment in the organizations where control metrices like ISO standards are taken into consideration to keep the requirement update. Annual checks need to be performed, with changes in laws and technology, applications used, the internal processes needs to be updated.

In this chapter, the thesis has tried to give an overview of the principles laid down in the GDPR, direct and indirect obligations on the data controllers stated in the GDPR and the obligations arising on data controllers as an effect of rights of data subjects acknowledged under chapter III.

In the next chapter of the thesis, this thesis intends to analyze the obligations on data controllers and the rights of data subjects on the tenets of proportionality, necessity and balancing of Fundamental rights.

Chapter IV

Analysis: Balancing of Rights

4.1 Fundamental Rights and the GDPR

The idea of protection of personal data within Europe can be traced to the Right to Private Life as stated under article 8[147] of the European Convention on human rights (ECHR). The ECHR came into force in 1950 and it included the right to respect for private life. The ECHR provides that everyone has respect for his or her private and family life, home and correspondence.[148] The said article not only affirms the right to personal data protection, but it also outlines the essential values embedded within it.[149] However, article 8 ECHR consists of general prohibition on interference while subject to certain public interest criteria that can justify interest in certain cases.[150]

The Charter on Fundamental Rights under article 8[151] guarantees the Right to Protection of personal data. The ECHR under art 8(2) lays down the basis of processing of personal data. In other words, every individual is entitled to have their personal information protected, used in a fair and legal way, and made available to them when they ask for a copy and if an individual feels that their personal information is wrong, they are entitled to ask for that information to be corrected.[152] Furthermore article 16[153] of the TFEU states that everyone has the right to protection of personal data concerning them.[154] Article 16 TFEU requires the legislator to lay down rules relating to the protection of individuals about the processing of personal data also in the areas of judicial co-

[147]European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 8.
[148] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 18..
[149] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 19.
[150] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 19.
[151]European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 7
[152] Available at: https://www.courts.ie/data-protection-what-are-my-rights#:~:text=Article%208%20of%20the%20EU%20Charter%20of%20Fundamental%20Rights%20states,basis%20laid%20down%20by%20law.
[153] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, at. 16.
[154] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, art 16(1); https://lexparency.org/eu/TFEU/ART_16/ last visited Nov 7, 2022.

operation in criminal matters and police co-operation, covering both cross-border and domestic processing of personal data."[155]

This requirement laid down under art. 16 of the TEFU[156] can be seen in various GDPR articles. Article 1(2) states that the GDPR protects fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. At the very outset the GDPR, clearly echoes that the provisions are aimed at protecting the rights and freedom of individuals. Moving forward, art. 2(2)(d) enshrines provision that excludes processing by competent authorities for criminal law enforcement, which is covered by the Law Enforcement Directive but still aligns with Article 16 TFEU's broader mandate. Art. 6 of the GDPR sets out lawful bases for processing personal data, including compliance with legal obligations and public interest, relevant to judicial and law enforcement contexts. This clearly restricts the data controllers to process data in manners which violated individual's right to privacy. Furthermore, art. 23 allows for restrictions on data subject rights when necessary for law enforcement, judicial independence, and national security, provided such restrictions are lawful and proportionate. This creates a balance between the FR of one individual against the greater good of society.

In EU legal order data protection is recognised under Fundamental Right, Human Right and also as a distinct law.[157] The Right under art. 8 ECHR and of protection of personal data strive to protect the values of autonomy and human dignity by granting individuals personal space to grow their personalities and shape their opinions.[158] The two also differ in their scope as art. 8 ECHR consists of general prohibition on interference subject to public interests whereas protection of Personal data is viewed as a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data is processed.[159]

[155] Ibid
[156] Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/1, art 16.
[157] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 19.
[158] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 19.
[159] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 19.

The GDPR strengthens the Right to Privacy as enshrined in the ECHR and the Charter. The court in the case of *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA v. Gegevensbeschermingsautoriteit*[160] under para 67 lays down that;

"Article 7 guarantees that everyone has the right to respect for his or her private and family life, home and communications, whereas article 8(1) of the Charter, like article 16(1) TFEU, expressly recognises that everyone has the right to the protection of personal data concerning him or her. It is clear from article 51(1) of Regulation 2016/679 that the supervisory authorities are responsible for monitoring the application of that regulation, for the purpose, inter alia, of protecting the fundamental rights of natural persons as regards the processing of their personal data."

In the case of *B v. Latvijas Republikas Saeima*[161] the CJEU under para 74 stated that, "article 10 of the GDPR is intended to ensure enhanced protection as regards processing which, because of the particular sensitivity of the data at issue, is liable to constitute a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by articles 7 and 8 of the Charter."

However, in the same case the CJEU has acknowledged that the rights are not absolute and can be curtailed under certain circumstances. In the case[162] the court stressed upon imposing limitations of the Rights of protection of personal data only in rare cases, "As recital 39 of the GDPR makes clear, that requirement of necessity is not met where the objective of general interest pursued can reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed in articles 7 and 8 of the Charter, since derogations and limitations in relation to the principle of protection of such data must apply only in so far as is strictly necessary".[163]

Further in the case[164] the CJEU stated that "It should be borne in mind that the fundamental rights to respect for private life and to the protection of personal data are not absolute rights but must be considered in relation to their function in society and be weighed against other fundamental rights. Limitations may therefore be imposed, so long as, in accordance with article 52(1) of the Charter,

[160]Case C-645/19 *Facebook Ireland Ltd v Gegevensbeschermingsautoriteit* ECLI:EU:C:2021:483.
[161]Case C-439/19 *Staatssecretaris van Justitie en Veiligheid v B* ECLI:EU:C:2021:504, para 74.
[162] Case C-439/19 *Staatssecretaris van Justitie en Veiligheid v B* ECLI:EU:C:2021:504, para para 110.
[163] Case C-439/19 *Staatssecretaris van Justitie en Veiligheid v B* ECLI:EU:C:2021:504, para 110.
[164] Case C-439/19 *Staatssecretaris van Justitie en Veiligheid v B* ECLI:EU:C:2021:504, para 105.

they are provided for by law, respect the essence of fundamental rights and observe the principle of proportionality. Under the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the European Union or the need to protect the rights and freedoms of others. They must apply only in so far as is strictly necessary and the legislation which entails the interference must lay clear and precise rules governing the scope and application of the measure in question.

To sum up, it can be said that the very essence of GDPR is based on protecting the Right to Privacy and Right to Data Protection as acknowledged under art. 7 and art. 8 of Charter on Fundamental Rights. This clearly states that the GDPR aims to protect the Fundamental Rights acknowledged and the provisions of the GDPR will ensure compliance to the FR. Under art. 6 of the GDPR, which lays down the six lawful basis of processing, it must be ensured that the right to privacy and right to data protection is not infringed. The processing of personal data must adhere to the principles of necessity and proportionality, while deciding a clear lawful basis for processing. In the case of processing of sensitive personal data, the CJEU through numerous cases has highlighted that processing of sensitive personal data must balance the freedom of information which is acknowledged under art 13 and 14 of the GDPR.

Article 12-15 of the GDPR, which emphasizes Right to Access, giving individuals more control over the processing of their personal data, upholds the right under art. 8 (2) of the Charter on FR, meaning that the right to access is important for control over personal data and for enforcement of rights. Right to rectification under art 16, protects accuracy of personal data ensuring dignity and autonomy under Art 8 of the Charter. The Right to erasure under Art. 17, gives the data subject more control over their data and autonomy to stop processing of personal data where it is not lawfully required. The Right to Object under art. 21 uploads art. 7 and 8 of the charter but restricts unwanted processing of personal data.

Art. 24 of the GDPR which lays down general obligations, and art. 25 which talks about Design and Default (DPbDD), upholds Art. 8 by laying obligation on data controllers to protect personal data. The FR principles have an overarching effect through art 45-49, in case of cross border transfers, ensuring that the personal data of EU residents governed by the GDPR must get the same level of protection outside the EU as well. Through the DPIA impact assessment the GDPR evaluates the risks to rights and freedoms of individual upholding art. 8 and art 52 of the Charter.

The above analysis clearly states that the GDPR is aligned with the objective of upholding the fundamental rights.

The GDPR is deeply rooted in the protection and promotion of fundamental rights, particularly the right to privacy and the protection of personal data as enshrined in article 8 of the Charter of Fundamental Rights of the European Union and article 16 of the TFEU. The GDPR does not merely regulate data processing as it affirms that such processing must always respect the dignity, autonomy, and freedom of individuals. It incorporates principles such as lawfulness, fairness, and transparency, ensuring that individuals are informed and empowered regarding how their data is used. The regulation also enforces purpose limitation, data minimization, and accountability, which collectively prevent arbitrary or excessive data use. Moreover, it provides enforceable rights, such as the right to access, rectify, erase, and object to processing which reflect the EU's commitment to upholding personal freedoms in the digital age. By embedding these safeguards, the GDPR operationalizes fundamental rights within a practical legal framework, ensuring that technological advancement does not come at the cost of individual liberties. This alignment with fundamental rights is further reinforced by the jurisprudence of the CJEU, which consistently interprets data protection laws in light of human rights principles.

4.2 Analysing the principle of proportionality and necessity in the GDPR

The GDPR is one of the most significant and prominent examples of proportionality's integration into EU secondary law. The discussions on GDPR have constantly highlighted the need to balance individual rights to privacy and data protection with the legitimate interests of controllers, and the functioning of the internal market. However, the text of the GDPR, clearly states that it is aimed at protecting individual's right to privacy.

In the subsequent paragraphs, we will analyze the whether the sub principles of proportionality can be inferred from the provisions of the GDPR.

At the outset, article 5[165] of the GDPR largely embeds the principle of proportionality in the GDPR. Art. 5(1)(a) lays down the requirements of lawful, fair and transparent processing of personal data which in itself lays down that the processing of personal data should be balanced and justified, emphasizing proportionality.

The GDPR does not define the term lawful, fair or transparent in this regard but when read with recital 4[166], it lays down 3 things:

- the idea is to serve individuals, meaning the focus is safeguard individuals,
- the second is that protection of personal data is not an absolute right and the principle of proportionality must be adhered to while applying the provisions mentioned therein, and
- third to respect all the fundamental rights and have proportional application of right to protection of personal data.

When reading this, the first bout of information is the priority to protect individuals' personal data but then in the second line, it emphasizes on balancing or rights and adhering to principle of proportionality.

The requirement of fair, transparent and lawful processing is directly reflected in the rights provided to data subjects under Chapter 3. The data controller is obligated to be fair and transparent when processing data and meeting the requirements of Chapter 3. In context of Right Access, the obligation is on data controller to be transparent when giving information requested by data subject, in terms of right to object, the data controller must be fair and restrict processing when requested.

The principle of proportionality can further be claimed in the concept of data minimization acknowledged under art. 5(1) (c). '*Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed',* this is how the aforementioned article lists the requirements for data minimization. In other words, data cannot and should not be used for a

[165] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 5.
[166] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, recital 4.

purpose for which it was not collected. The controller have a requirement to conduct a lawful basis of processing to determine the purpose of processing. If the processing involves using data for a purpose outside what was assessed when the lawful basis was conducted, the controller will be liable for no- compliance of the provisions of the GDPR. If the processing is outside what can be reasonably expected by the data subject whose personal data is being processed, then the data controller will be held for non-compliance.

The principle of data minimization can also be reflected under art. 17[167] Right to Erasure and art. 18[168], Right to restriction of processing. The sub principle of proportionality which is 'necessity' aims processing what is absolutely necessary to be meet the purpose of processing. It is inclined at reducing the use of excessive data or excessively using the data without a lawful basis, it also empowers the individuals to request.

Similarly the principle of storage limitation under art. 5(1) (e) which lays down the obligation for storing data only for a limited time frame, reflects temporal proportionality. Temporal proportionality refers to the principle that personal data should only be retained for as long as necessary to fulfill the purpose for which it was collected. It is an obligation on data controller and lays down proportional processing of data but at the same time it is strategic and time bound. This is reflected very well under the Right to Erasure, which acknowledges that the data subjects have the right to request erasure.

The key aspects here is that the data controller must define retention period for different processing purposes and moreover justify the retention period. Retention is often assessed from other regulations applicable like labour laws, employment regulations, etc. This lays down the principle of proportionality for use of personal data of data subjects. However, at the same time it is on the data controllers to research and establish a lawful retention period, keeping several other regulations like AML[169], sanctions, pensions, labour laws, payroll requirements, in consideration.

[167] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 17.
[168] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 18.
[169]Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2024] OJ L212/1.

The storage limitation brings in another obligation on the data controller, which is of retaining the data. Once the purpose of processing is over and there is no longer the need to process personal data, the data needs to be archived, retained in a form and place where it is not accessible easily and should be used in any kind of processing. Retaining data can require a huge cost on data controllers as it is likely to need technical developments and advanced tools.

It is true that the principle of proportionality is reflected in storage limitation but the responsibilities on data controllers are not proportional. The controller has to undertake several measures, develop complicated procedures to ensure that no processing carried out while the data is in retention period before the Right to Erasure kicks in.

The next article where proportionality stands strong with it's sub principle '*proportionality stricto sensu*' is article 6 (1) (f) of the GDPR. The Right to object under article 21 is directly related to processing based on legitimate interest. The data subjects have the right to seek restriction of processing based on legitimate interest. Another aspect of proportionality is balancing of rights and art. 6(1) (f) requires balancing of rights of data subjects against others.

The test of balancing expands to the rights provided under chapter 3 of the GDPR where in under art. 15 (4) when a data subject's right to access exceeds its limits to infringe other people's right it shall not be met. In case of Right to restriction of processing article 17(3) outlines exceptions, including:

- When processing is necessary for freedom of expression and information.
- For compliance with legal obligations.
- For reasons of public interest (e.g., public health).
- For establishment, exercise or defense of legal claims.

These exceptions reflect a balance of the individual's right to erasure against other societal or legal interests.

The principle of proportionality is not only limited to Chapter III of the GDPR, it extends to chapter IV of the GDPR, which lays down the obligations on data controllers to meet the obligations and compliance under the GDPR. The Data Protection Impact Assessments (DPIA) under art.35 operationalize balancing by requiring an advanced level of assessment of risks and laying down mitigating actions. This embeds a *rational weighing process* into legal compliance. In case of DPIA, the test of proportionality no longer remains a mere principle but becomes more real,

operational and an essential part of governance. This lays down an obligation on data controllers demanding transparency, justification, and careful calibration of measures that interfere with rights.

From the analysis made above, the principle of proportionality and the sub principles namely suitability, necessity, and proportionality stricto sensu which support in assessing the principle are part of the black letter regulation. The obligations put on data controllers under Chapter III and Chapter IV are suitable to ensure compliance with the GDPR and to protect the processing of individual personal data. The provisions suitably give individuals more power over the processing of their personal data. The assessments in lawful basis analysis, DPIA, TIA, organizational and technical measures are suitable to ensure protection of personal data while it is with the data controller. The principle of necessity is also explicitly highlighted by the provisions in data minimization and storage limitation. The third sub principle called proportionality *stricto-sensu* is also reflected through various balancing principles where proportionality is interpreted in the strictest sense.

As we read in chapter 2 of this thesis, the principle of necessity is also a sub principle of proportionality. The principle of necessity adds substantive as well as procedural limitations. The principle of necessity requires that nothing more than what is absolutely necessary should be done. It limits the processing of data including the purpose of processing, retention and deletion of data access of data to what is necessary and not in excess infringing other's rights. The principle of necessity requires:

- Less intrusive ways to achieve the same legitimate aim;
- The chosen measure is suitably customized and effective; and
- The interference with rights is justified by clear, and justifiable reasoning.

At the outset the principle of necessity can be traced in art. 5, which states that data should be processed in a fair, lawful and transparent manner. If we look at art. 9 of the GDPR, it requires explicit justification for processing sensitive personal data, enforcing one of the sub-principles of necessity. Under Chapter 3 of the GDPR, the Right to Access, under art.15 specifies while sharing information about one's personal data, another person's personal data should not be shared,

meaning the use of less intrusive way to share data without infringing the rights of others. Under the Right to Erasure, art. 17, the third sub principle of necessity is highlighted. When the data controller sets retention period before deleting personal data of data subjects, the period of retention stated or being followed by an organization must be justified with clear reasoning. In this case the data controller can use requirements from other laws including AML, sanctions, payroll, labor market regulations, securities regulations, regulations on health data to justify the period of retention before deletion. In case of right to object under art. 21, the data subject can object to processing of personal data if the chosen measure is not suitable for processing such data, for example in case of sensitive personal data, the technical measures, impact assessments must be done in way to indicate that the processing involves high risk. Under art. 18 of the GDPR, the data subject can restrict processing which is not lawfully needed but such data can be retained for legal claims and other relevant purposes. In this case, all three sub principles of necessity come into play. In other words, the processing is not needed, thus a less intrusive way to achieve the aim would be restricting processing and keeping the data archived for any use, the method is suitable in cases where there is no requirement of processing and in order to keep processing that information, the data controller must justify the requirements.

The principle of necessity and its sub principles are also highlighted in chapter IV of the GDPR. Article 24[170] of the GDPR, lays down a general obligation to have technical and organizational measures established. The principle of necessity here is highlighted in the fact that only what is necessary should be processed, similarly proper security measures should be in place to protect the personal data in control of data controllers. Similarly, under art. 25[171] which lays down the foundation for Privacy by design and default data ccontrollers must implement measures to ensure that only necessary personal data is processed. This eembeds proportionality into system design.

Thus, Necessity as a principle governs the GDPR. It is reflected in general sections, in the acknowledgement of rights to data subjects and also in the obligations under chapter IV to data

[170] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 24.
[171] Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 25.

controllers. Apart from that, the principle of necessity is deeply embedded in the concept of lawful basis of processing which is the very first step for processing personal data for a data controller.

It is natural to state that the principle of balancing which includes proportionality, necessity and alignment with fundamental rights are the core of the GDPR. At the outset the GDPR has stated its allegiance to working for fundamental rights of individuals and it can be seen in multiple articles listed above. The principles of proportionality and necessity form an integral part of the GDPR. The obligation on data controllers to be proportional to the purpose while processing data and documenting that such processing is necessary to provide the service or meet the requirements of the contract is established in the GDPR. The controller cannot process data which is more than necessary to meet the requirements of the contract or service. The GDPR carefully lays down the principle of proportionality and necessity in provisions of the GDPR.

4.3 Observations and suggestions

The principle of balancing is present in the GDPR provisions. The legislation is well balanced to protect the rights of data subjects and also give discretion to data controllers on how they meet the requirements. However, it is a bit of a different story when the legislative requirements are put into operational work. The data controllers in almost all cases are either providing services or products for which they use personal data. The impact assessments and the risk assessments that need to be carried out is quite a complex process for data controllers to establish and then continue. The process needs to be developed with the development in interpretation of the legislation. The regulation is a living document and with new interpretations the obligation on controller increases to include the new requirements stemming from the interpretation. For example, AI regulation is a new development, the provisions of which also affect data privacy operations. The AI Act calls for a Fundamental Rights Impact Assessment to be done which supplements a DPIA under art. 35 of the GDPR. It is for data controllers to update their DPIA, to make changes in tools to include this new requirement.

Another example is data breach notifications. The Finnish DPA has launched a new format for reporting breaches[172] which affect data controllers' obligations as now they have to update internal documents to meet the requirements of the new breach reporting format.

While the obligations on data controller is much higher practically, it is also important to ensure that personal data subjects is safe and all requisite measures are taken by data controllers to protect that dat. What could support the controllers is more guidance for local DPA, EU guidance and training for individuals and organizations. Having closed local forums for organizations to discuss the pertinent issues related to processing of personal data, implication of new cases or interpretation of the law, or must haves in cases processing sensitive personal data can support the organizations in being better informed.

[172] Data Breach Reporting, Finnish Data Protection Authority, available at https://tietosuoja.fi/en/data-breach-notification, last visited Nov 11, 2025.

Chapter V: Conclusion

The GDPR is a landmark in the evolution of data protection law and it empowers individuals with more control over their personal data while ensuring that data controllers, operate within a framework of accountability, transparency, and fairness. This thesis has analyzed, the reality of balancing these rights and obligations is far more complex than what is visible by simply reading the black letter of the regulation.

At the core of the GDPR lies a duality: the rights of data subjects and the obligations of data controllers. This duality is not merely theoretical; it transforms in the daily operations of organizations. The GDPR's principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability are operational requirements that shape the collection of personal data, processing of it, deleting personal data and storing it. For example, the Right to Erasure is not operationally applied by deleting data each time a data subject exercises his/her right to erasure. The obligation on data controllers to navigate a labyrinth of sector-specific laws such as employment, insurance, and anti-money laundering regulations that may require data retention for defined periods. The process demands organizational capabilities, technical infrastructure, and continuous training for employees. Similarly, in case of Right to Access, the controllers is obligated to provide data subjects with information in a readable and understandable format within 30 days. In large organizations, where data is scattered across multiple systems and may be encrypted or stored in the cloud, fulfilling this right requires significant investment in data management systems and employee expertise.

The thesis has traced the roots of the GDPR's balancing of rights to foundational principles of EU law: proportionality, necessity, and respect for fundamental rights.

The principle of proportionality requires that any limitation of rights or imposition of burdens be suitable to desired objectives. The GDPR's requirements for data minimization and storage limitation are direct expressions of this principle. For instance, controllers must justify the retention period for personal data, balancing the need for operational efficiency against the individual's right to privacy.

Necessity operates as a substantive shield against arbitrary intrusions into fundamental freedoms. Data controllers must demonstrate that no less intrusive measure could achieve the same objective.

Fundamental rights, particularly the right to privacy and data protection are the normative foundation of the GDPR. The Charter's art. 7 and 8, and the ECJ's case law, have transformed these rights from peripheral considerations to central constraints on legislative and executive action. art. 1 of the GDPR, at the outset states that the aim of the GDPR is to safeguard art, 7 and 8 of the Charter.

While the GDPR's text provides a robust framework for protecting individual rights, the operational realities for data controllers are far more demanding. The obligations extend beyond mere compliance; they require organizations to proactively demonstrate that their processes, systems, and human resources are equipped to facilitate data subject rights. The organizations must be equipped and have resources to meet the requirements of Right to Access, Right to Rectification, Right to Object, Right to Erasure.

Data controllers should have a process to provide access in time, correct inaccurate data but also ensure that corrections propagate across all systems and third-party processors. Process and training to handle the right to object to processing, especially for direct marketing or profiling. These puts place an obligation on data controllers to stop processing upon request. The Right to Erasure requires much more than simple deletion. Data controllers must assess retention periods, conduct DPIA, and ensure that archived data is secure and inaccessible for processing. The requisite technical and organizational measures should be in place to cater to this.

This clearly indicates that compliance with the obligations laid down in the GDPR require substantial investment by the organization, in training employees, creating reliable technical solutions, establishing processes, creating tools for impact assessments and have legal and compliance support.

The thesis has shown that the rights enshrined in the GDPR are not absolute. The ECJ and the EctHr have consistently held that limitations may be imposed, provided they are necessary, proportionate, and grounded in law. The balancing of interests is evident in cases involving requests for erasure, where the courts have weighed the individual's right to privacy against the individual's right to information. These cases stated in Chapter 2 and 3 of the thesis reinforce the

principle that data protection rights must be balanced against other fundamental rights and societal interests.

The main question of this thesis is whether the GDPR truly achieves a genuine balance between the rights of data subjects and the obligations of data controllers or is it just on paper. The analysis clearly depicts that while the regulation aspires to balance, in practice, the burden on controllers is substantial and often disproportionate. In other words, the analysis in chapter IV shows that the principle of proportionality, necessity and respect for FR are clearly embedded in the provisions but the practical aspects of implementing it on organizations is a different game which is far from balanced. Data controllers are compelled to navigate the complexity of multiple regulations, sectoral legal requirements, technical challenges, and operational constraints. The cost of compliance developing processes, training staff, investing in technology, and managing data subject requests is significant, particularly for small and medium-sized enterprises. The risk of non-compliance is equally high, leading to financial damage, reputational damage and risk of business continuity.

At the same time, data subjects enjoy strong rights and vigilant avenues for redress. They can access, rectify, object to, and erase their data, often with minimal justification. The courts have generally favored the protection of individual rights, imposing strict standards on controllers. However, the rights of data subjects are not absolute. The GDPR has recognize the need for exceptions, particularly where other fundamental rights or public interests are at stake. The balancing act is ongoing, shaped by evolving jurisprudence, technological change, and societal expectations.

The principles of proportionality, necessity, and respect for fundamental rights provide a solid foundation for balancing competing interests. However, the operational burden on data controllers is considerable. To achieve a more equitable balance, policymakers and regulators should consider:

1. Providing elaborate, more practical guidance on implementing rights and obligations for organizations.
2. Promoting dialogue by providing a forum for discussion, raising concerns and seeking guidance between regulators, and controllers, to identify challenges, share best practices, and adapt to emerging risks.

The journey through the GDPR's provisions, principles, and case law reveals a dynamic and evolving landscape. The regulation is a living document, and it is shaped by judicial interpretation, regulatory guidance, and the practical realities of implementation. The balance between the rights of data subjects and the obligations of data controllers is not a fixed point but a moving target, responsive to new challenges and opportunities. As data continues to drive innovation and economic growth, the importance of safeguarding individual rights while enabling responsible data use will only increase. The GDPR provides a robust framework for this, but its true test lies in its application.

In conclusion, the GDPR is both a shield and a sword: a shield for individuals seeking to protect their personal data, and a sword for organizations striving to demonstrate accountability and compliance. The balance is delicate, demanding constant attention, adaptation, and commitment from all stakeholders. The future of data protection in Europe and beyond will depend on our collective ability to uphold this balance in the face of rapid change.

BIBLIOGRAPHY

Legislation and Official Documents

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.
- Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) [2005] OJ L149/22.
- Regulation (EU) 2016/679 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 and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
- Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1.
- Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act) [2023] OJ L, forthcoming publication.
- European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 7.
- European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 8.
- Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, art 16(1).

Cases

- Case C-112/00 Schmidberger v Austria [2003] ECR I-5659.
- Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C:2014:317, [2014] OJ C 212/4.
- Case C-136/17 GC and Others v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:773, [2019] OJ C 424/8.
- Case C-331/88 The Queen v Minister of Agriculture, Fisheries and Food, ex parte Fedesa and others [1990] ECR I-4023.
- Case C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni ECLI:EU:C:2017:197.
- Case C-439/19 Staatssecretaris van Justitie en Veiligheid v B ECLI:EU:C:2021:504.
- Case C-645/19 Facebook Ireland Ltd v Gegevensbeschermingsautoriteit ECLI:EU:C:2021:483.
- Węgrzynowski and Smolczewski v Poland, App no 33846/07 (ECtHR, 16 July 2013).
- Mediengruppe Österreich GmbH v Austria, App no 37713/18 (ECtHR, 28 April 2022).
- Stauder v City of Ulm, Case 29/69 [1969] ECR 419.
- Internationale Handelsgesellschaft, Case 11/70 [1970] ECR 1125.
- Nold v Commission, Case 4/73 [1974] ECR 491.
- Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others, Case C-293/12 [2014] ECLI:EU:C:2014:238.
- Maximillian Schrems v Data Protection Commissioner, Case C-362/14 [2015] ECLI:EU:C:2015:650 (Schrems I).

- Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18 [2020] ECLI:EU:C:2020:559 (Schrems II).
- Peter Nowak v Data Protection Commissioner, C-434/16 ECLI:EU:C:2017:994.
- Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others [2016] ECLI:EU:C:2016:970.
- Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others [2020] ECLI:EU:C:2020:791.

Books and Academic Articles

- European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law (2018 edn, Publications Office of the European Union 2018).
- Takis Tridimas, The General Principles of EU Law (2nd edn, Oxford University Press 2006).
- Tor-Inge Harbo, The Function of Proportionality Analysis in European Law (Brill Nijhoff 2015).
- Jan-R Sieckmann (ed), Proportionality, Balancing, and Rights: Robert Alexy's Theory of Constitutional Rights (Springer Nature Switzerland AG 2021).
- Koen Lenaerts, 'Exploring the limits of the EU Charter of Fundamental Rights' (2012) 8 European Constitutional Law Review 375.
- Eduardo Ustaran (ed), European Data Protection: Law and Practice (2nd edn, IAPP 2019).
- IT Governance Privacy Team, EU GDPR: An Implementation and Compliance Guide (4th edn, IT Governance Publishing 2020).

- Emily Crawford, 'Proportionality' (Oxford Public International Law, last updated May 2011) <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1446> accessed 27 October 2025.
- Richmond Chambers, 'The Principle of Proportionality in EU Law – Part 1' (Richmond Chambers, 21 February 2022) <https://www.richmondchambers.com/news/the-principle-of-proportionality-in-eu-law-part-1/> accessed 27 October 2025.

Guidelines and Reports

- Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679, WP260 rev.01, adopted on 29 November 2017, revised and adopted on 11 April 2018.
- Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, adopted on 9 April 2014.
- Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 rev.01, adopted on 3 October 2017, revised and adopted on 6 February 2018.
- European Data Protection Board, Guidelines 01/2022 on Rights of Data Subjects: Right of Access, Version 2.0, adopted on 28 March 2023.
- European Data Protection Board, Guidelines 4/2019 on Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020.
- European Data Protection Board, Guidelines 5/2019 on the criteria of the Right to be Forgotten in search engines cases under the GDPR (Part 1), Version 2.0, adopted on 12 July 2019.
- European Data Protection Supervisor, Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit (11 April 2017).

- Office of the Data Protection Ombudsman (Finland), Guidelines for Data Protection Impact Assessment (DPIA), 2021 <https://tietosuoja.fi/en/data-protection-impact-assessment> accessed 27 October 2025.
- European Commission, A Digital Agenda for Europe: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2010) 245 final, Brussels, 19 May 2010.
- European Commission, Second Report on the Application of the General Data Protection Regulation, COM(2024) 482 final, Communication from the Commission to the European Parliament and the Council, Brussels, 25 July 2024.
- European Commission, 'Antitrust: Commission fines Apple €1.1 billion for anti-competitive practices in the distribution of Apple Pay' IP/20/1163, 16 June 2020, 1 <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_1163/IP_20_1163_EN.pdf> accessed 24 March 2025.
- European Parliament, 'Digital Agenda for Europe' (Fact Sheets on the European Union) <https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe> accessed 2 June 2025.
- Alessandro Mantelero, 'One-Stop-Shop Thematic Case Digest – Right to Object' (GDPRhub, 9 December 2022) <https://gdprhub.eu/Thematic_Case_Digest:_Right_to_Object>

Websites and Online Resources

- GDPRhub, 'Article 5 GDPR – Principles relating to processing of personal data' (GDPRhub) <https://gdprhub.eu/Article_5_GDPR> accessed 27 October 2025.
- GDPRhub, 'Article 16 GDPR – Right to rectification' (GDPRhub) <https://gdprhub.eu/Article_16_GDPR> accessed 27 October 2025.
- GDPRhub, 'Article 17 GDPR – Right to erasure ("right to be forgotten")' (GDPRhub) <https://gdprhub.eu/Article_17_GDPR> accessed 27 October 2025.

- GDPRhub, ‘Article 21 GDPR – Right to object’ (GDPRhub) <https://gdprhub.eu/Article_21_GDPR> accessed 27 October 2025.
- GDPRhub, ‘Article 24 GDPR – Responsibility of the controller’ (GDPRhub) <https://gdprhub.eu/Article_24_GDPR> accessed 27 October 2025.
- GDPRhub, ‘Article 30 GDPR – Records of processing activities’ (GDPRhub) <https://gdprhub.eu/Article_30_GDPR> accessed 20 March 2024.
- Principle Defence, ‘Your GDPR Rights Explained – The Right to Rectification’ <https://principledefence.com/your-gdpr-rights-explained-the-right-to-rectification/> accessed 27 January 2024.
- Information Commissioner’s Office, ‘What methods can we use to provide privacy information?’ (ICO) <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/what-methods-can-we-use-to-provide-privacy-information/> accessed 10 March 2023.
- Information Commissioner’s Office, ‘The Principle of Accuracy’ (ICO) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/> accessed 27 January 2024.
- Swedish Authority for Privacy Protection (IMY), Decision against Spotify AB regarding the right of access under the GDPR, Decision No. DI-2020-4061, 13 June 2023 <https://www.imy.se/en/news/spotify-receives-an-administrative-fine/> accessed 27 October 2025.
- Datatilsynet (Norwegian Data Protection Authority), ‘Decision against Komplett Bank ASA – Right to Object’ (GDPRhub) <https://gdprhub.eu/index.php?title=Datatilsynet_-_Komplett_Bank_ASA> accessed 27 October 2025.
- European Court of Human Rights and Court of Justice of the European Union, Joint Fact Sheet – Right to be Forgotten: ECtHR and CJEU Case-Law, last updated 28 February 2025 <https://www.echr.coe.int/documents/fs_right_to_be_forgotten_eng.pdf> accessed 27 October 2025.

- European Commission, ‘Data Act | Shaping Europe’s Digital Future’ (Digital Strategy, 2023) <https://digital-strategy.ec.europa.eu/en/policies/data-act> accessed 27 October 2025.