# Data subject rights in the era of AI. Can the right of rectification protect data subjects against incorrect inferences made by artificial intelligence systems?

Rute Silva Gomes
Data protection and IT lawyer
rute.silva.gomes@outlook.com
ORCID: 0009-0005-3651-5123

Reception: 04/11/2024
Acceptance: 26/12/2024
Publication: 26/06/2025

**Recommended citation:** SILVA GOMES, R. (2025). "Data subject rights in the era of AI. Can the right of rectification protect data subjects against incorrect inferences made by artificial intelligence systems?". *Quaderns IEE: Revista de l'Institut d'Estudis Europeus*, *4*(2), 85-111. DOI: <https://doi.org/10.5565/rev/quadernsiee.110>

## Abstract

The widespread use of AI and its increasing capabilities, as well as the impact of decisions made by AI systems on the lives of natural persons, have prompted discussions on the extent to which existing regulations are well equipped to deal with these systems.

In this context, we can ask what is the role of the right of rectification in protecting data subjects from incorrect inferences made by AI systems and to what extent this right could play a key role in protecting data subjects from those inferences.

To answer these questions, we propose to examine what rights are granted to data subjects under article 16 of the GDPR; what is the current state of play regarding the application of this right to inferences; to which extent should data subjects have a right to rectify or complete inferences about them made by AI systems; and what are the obligations and good practices that could be implemented to facilitate the exercise of this right in the aforementioned context.

We argue the right to rectification may indeed be key to challenging inferences made by AI systems, provided there is a clear and consistent interpretation of its scope and the obligations it entails.

**Keywords:** GDPR; Right of rectification; Artificial intelligence; Inferences, AI systems.

**Resumen.** *Derechos de los interesados en la era de la IA. ¿Puede el derecho de rectificación proteger a los interesados contra interferencias incorrectas realizadas por los sistemas de Inteligencia Artificial?*

El uso generalizado de la IA y sus crecientes capacidades, así como el impacto de las decisiones tomadas por los sistemas de IA en la vida de las personas físicas, han suscitado debates sobre hasta qué punto las normativas existentes están bien equipadas para hacer frente a estos sistemas.

En este contexto, podemos preguntarnos cuál es el papel del derecho de rectificación en la protección de los interesados frente a las inferencias incorrectas realizadas por los sistemas de IA y en qué medida este derecho podría desempeñar un papel clave en la protección de los interesados frente a estas inferencias.

Para responder a estas preguntas, proponemos examinar qué derechos se conceden a los interesados en virtud del artículo 16 del RGPD; cuál es la situación actual en lo que respecta a la aplicación de este derecho a inferencias; en qué medida los interesados deberían tener derecho a rectificar o completar las inferencias sobre ellos hechas por sistemas de IA; y cuáles son las obligaciones y buenas prácticas que podrían aplicarse para facilitar el ejercicio de este derecho.

Sostenemos que el derecho de rectificación puede ser realmente clave para impugnar las inferencias realizadas por los sistemas de IA, desde que exista una interpretación clara y coherente de su alcance y de las obligaciones que esto derecho conlleva.

**Palabras clave:** RGPD; Derecho de rectificación; Inteligencia artificial; Inferencias; Sistemas de IA.

**Resum.** *Drets dels interessats a l'era de la IA. El dret de rectificació pot protegir els interessats contra interferències incorrectes realitzades pels sistemes d'intel·ligència artificial?*

L'ús generalitzat de la IA i les seves capacitats creixents, així com l'impacte de les decisions preses pels sistemes d'IA a la vida de les persones físiques, han suscitat debats sobre fins a quin punt les normatives existents estan ben equipades per fer front a aquests sistemes.

En aquest context, ens podem preguntar quin és el paper del dret de rectificació en la protecció dels interessats davant de les inferències incorrectes realitzades pels sistemes d'IA i en quina mesura aquest dret podria tenir un paper clau en la protecció dels interessats davant d'aquestes inferències.

Per respondre aquestes preguntes, proposem examinar quins drets es concedeixen als interessats en virtut de l'article 16 del RGPD; quina és la situació actual pel que fa a l'aplicació d'aquest dret a inferències; en quina mesura els interessats haurien de tenir dret a rectificar o completar les inferències sobre aquests fets per

sistemes d'IA; i quines són les obligacions i les bones pràctiques que es podrien aplicar per facilitar l'exercici d'aquest dret.

Sostenim que el dret de rectificació pot ser clau per impugnar les inferències realitzades pels sistemes d'IA, des que hi hagi una interpretació clara i coherent del seu abast i de les obligacions que això comporta.

**Paraules clau:** RGPD; Dret de rectificació; Intel·ligència artificial; Inferències; Sistemes d'IA.

**Summary**

1. Introduction

2. The right of rectification

3. State of the art in the application of the right of rectification to inferences

4. Right of rectification and AI systems – applicability and specific challenges

5. Right of rectification and AI systems – possible solutions

6. Conclusion

7. Bibliography

## 1. INTRODUCTION

Throughout the last years, the increased use (McKinsey Analytics, 2019) and capabilities (Singla et al., 2024) of artificial intelligence (AI)[1] prompted many discussions on its benefits, risks and need of regulation. Many have highlighted the benefits of AI, which has the potential to solve some of the world's biggest challenges (European Commission, 2018), while others pointed out its risks (European Commission, 2020), from bias, discrimination and economic inequality (Marr, 2023) to, in more grim scenarios, the risk of humans' extinction (Egan, 2024).

These concerns, normally accompanied by a call to regulate AI, echoed in institutions with legislative powers[2] and, particularly in the European institutions. In fact, more than five years ago, in 2018, the Commission noted that AI was already part of our lives, from the use of "virtual personal assistant to organize our working day, to travelling in a self-driving vehicle, to our phones suggesting songs or restaurants that we might like, AI is a reality", stating the need for an appropriate legal framework for AI (European Commission, 2018), and, before that, the European Council had already stressed the urgency of addressing emerging trends, such as "artificial intelligence and blockchain technologies, while at the same time ensuring a high level of data protection, digital rights and ethical standards" (European Commission, 2018, p. 3). These calls to action led the Commission to propose the first legal framework on AI in

[1] For the purposes of this article, we will not enter the discussion on what should be defined as AI, rather using the definition of AI system included in article 3(1) of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[2] As of the date of writing of this article, more than thirty countries have passed laws mentioning AI, even though with different approaches (Gutiérrez, 2024).

2021[3] and culminated in the recent approval of the AI Act[4], the "world's first comprehensive AI law" (European Commission , 2024).

Consequently, the approval of this regulation led both professionals and academics to focus on the new provisions aimed at regulating AI, or, as it has been mentioned, to a state of "AI hype" (Wiewiórowski, 2024b) or "everything AI" (Wiewiórowski, 2024a). However, as it has been rightfully noted, "the EU AI Act also does not apply in a vacuum as it is part of a broader legal framework that contains provisions to protect individuals from the misuse of AI systems" (Wiewiórowski, 2024a), and, while this regulation aims to govern the placing on the market, putting into service and use AI systems,[5] these systems shall also comply with other European rules and, in particular, where personal data is processed, with those relating to the processing of personal data.[6]

Regarding, in particular, data subject rights, recital 10 of the AI Act notes that:

> It is also appropriate to clarify that data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law, including the rights related to solely automated individual decision-making, including profiling. Harmonised rules for the placing on the market, the putting into service and the use of AI systems established under this Regulation should facilitate the effective implementation and enable the exercise of the data subjects' rights and other remedies guaranteed under Union law on the protection of personal data and of other fundamental rights.

Therefore, the data subject rights set forth in the General Data Protection Regulation[7] (GDPR, hereinafter) will, or at least, should, play a relevant role in protecting data subjects where personal data is processed in the context of the training, validation, deployment or operation of AI systems (Agencia Española de Protección de Datos, 2020), particularly where the use of these systems may lead to incorrect conclusions.[8]

It has however been recognized that the exercise and respect for data subject rights within the context of AI is not free of challenges, on the contrary, as we will see below, it generates many doubts regarding their practical implementation in the context of AI.

---

[3] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts (COM/2021/206 final).

[4] Echoing the consideration of both the benefits and risks of AI in general, see recitals 4 and 5 of the AI Act.

[5] Article 1(2)(a) of the AI Act.

[6] Article 1(7) of the AI Act.

[7] 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

[8] Inaccuracy has, in fact, been recognized as the most experienced risk of the use of generative AI (Singla, Sukharevsky, Yee, Chui, & Hall, 2024).

In this article, we propose to focus, specifically, on the right of rectification included in article 16 of the GDPR and, within this context, on the extent to which this right may be used to react to incorrect inferences made by AI systems.

To this end, part 2 of this article will begin to describe the right of rectification set forth in article 16 of the GDPR, this being followed by part 3, in which we will analyse existing guidelines and jurisprudence relating to the right of rectification. Thereafter, part 4 will explore to which extent the right of rectification can be exercised within the context of AI systems, as well as the existing challenges and limitations that emerge in this context, especially when we consider the possibility of resorting to the right of rectification to challenge incorrect inferences made by AI systems. We shall conclude with some remarks, in part 5, regarding what could be done to ensure the right of rectification can be effectively exercised within the context previously analysed.

Our work shall rely mainly on doctrinal legal analysis, as our aim is to interpret and determine the limits and limitations of article 16 of the GDPR, considering therefore not only the GDPR and relevant case law, but also secondary legal literature and official documents of institutions of the European Union (particularly the guidelines issued by the European Data Protection Board, the European Data Protection Supervisor and national supervisory authorities).

## 2. THE RIGHT OF RECTIFICATION

According to article 16 of the GDPR:

> The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Therefore, the right of rectification is, in fact, composed of two rights. On the one hand, data subjects may rectify their personal data. On the other hand, they may also complete personal data relating to them that they consider is incomplete.

This right is not a novelty, as article 12(b) of the Data Protection Directive[9] already established that Member states should guarantee that data subjects had the right to obtain from the controller the rectification of their data which was incomplete or inaccurate. Likewise, this right was already part of Convention 108,[10] being established in article 8(c) of it that any person should be enabled "to obtain, as the case

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

[10] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

may be, rectification or erasure of such data", this right being then maintained in article 9(e) of the modernised text of the Convention.[11]

Furthermore, there is a clear connection between this right and the principle of accuracy set forth in article 5 (1) (d) of the GDPR (Ustaran, 2019), under which personal data shall be accurate and kept up to date, further being required from controllers to take every reasonable step to ensure that inaccurate personal data are rectified without delay, this assessment being made considering the purposes for which personal data are processed. It can also be said that this right depends on the transparency obligations laid down in the GDPR and on the effective exercise of the right of access, as the identification of incorrect or incomplete data naturally depends on the ability to identify such data.

Moving to the analysis of the exact content of the right of rectification, it can be concluded, from the analysis of articles 16 and 5(1)(d) of the GDPR, that not only data subjects have the right to correct and complete their data, but also that once it becomes apparent to the controller, or the controller is made aware by the data subject (ICO, s.d.), through the exercise of the right of rectification, that certain personal data it processes is not correct or complete, the controller shall take all reasonable steps to correct or complete the data without delay.

It should be noted that the GDPR does not define accuracy. Considering, however, the guidelines on automated individual decision-making and profiling issued by the Article 29 Data Protection Working Party (WP29) (Article 29 Data Protection Working Party, 2018) and, particularly, the reference made, within the section relating to the right of rectification, to the fact that input data "may be inaccurate or irrelevant, or taken out of context" (Article 29 Data Protection Working Party, 2018, p. 17), it appears that a distinction is drawn between data that is inaccurate and data that is misleading.

Therefore, it could be questioned whether the right of rectification applies solely to inaccurate data, thus excluding situations in which certain data, albeit correct, is considered in such a way that is misleading. . As an example, a data subject could be the subject of proceedings relating to the payment of a debt, being thereafter considered, upon investigation, that the debt was not due by the data subject, but rather by a third party. In this case, while the information on the existence of these proceedings are factual correct, if a decision is taken considering solely this fact (the result of the proceedings being disregarded), the information considered for the formation of the decision could, considering the purpose of processing, be misleading. In our opinion, the answer to this question should be negative, rather being considered that while personal data that is misleading can be correct (in which case the first right granted under article 16 of the GDPR cannot be exercised), these data would be considered incomplete, in the sense that they do not adequately reflect reality, the data subject having the right to complete that data.

[11] Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

Furthermore, while from the wording of article 16 it appears that only the right to complete personal data and, therefore, only the notion of incompleteness, must be analysed considering the purposes of processing (Kuner, Bygrave, & Docksey, 2020, p. 473), article 5(1)(d) appears to indicate that the relevant purposes of processing should also be taken into account when assessing if the personal data is correct, conclusion supported by the judgement of the Court of Justice of the European Union (CJEU, hereinafter), in the decision of the *case Nowak*,[12] and by the European Data Protection Board (European Data Protection Board, 2024).

Consequently, the assessment on whether the personal data processed by the controller is complete or correct always depends on why personal data is being processed. In some cases, this is assessment is straightforward. For example, if the data subject's address is processed for delivering an order and the address is incomplete, it is clear the right to complete the address could be exercised.

However, where personal data is processed, for example, for profiling purposes, it could be less clear to which extent certain data needs to be corrected or completed, and while the data subject may consider that such action is necessary, the controller may on its turn consider that the information to be added is irrelevant. In these situations, and as it has been noted, it is not clear which of the perspectives shall prevail (Custers & Vrabec, 2024), and while it could be argued that both interpretations have their merits, the data subject having the right to provide a supplementary statement about the reasons why he or she considers the personal data is incorrect or incomplete, so that both views coexist in the database (Custers & Vrabec, 2024), the fact is that such a statement is only allowed were the data is not complete and, furthermore, such a solution does not grant data subjects control over their personal data. Furthermore, insofar as it is up to the controller to decide if the data needs to be corrected or completed, it must be concluded that the right of rectification is subject not only to the limitations allowed under article 23 of the GDPR, but also to limitations derived from the controller's opinion on what personal data is relevant for the applicable purpose of processing.[13]

On this matter, it is also worth highlighting that it has been considered that during civil litigation or proceedings before a public authority aimed at deciding whether the personal data is correct and complete, "the data subject can ask for an entry or note to be placed on his or her data file stating that the accuracy is contested and that an official decision is pending" (European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 221), the controller also having to refrain from presenting the contested personal data as correct until a decision on the correctness or completeness of the personal data is issued, particularly where these data is transferred to third parties.[14]

[12] Case C-434/16, Nowak, 2017, ECLI:EU:C:2017:994, para. 53.
[13] Opinion of Advocate General Collins in case C-247/23, Deldits, 2024, ECLI:EU:C:2024:747, para. 48.
[14] Once the decision is issued, and if it is concluded that personal data has to be rectified, the controller shall comply with article 19 of the GDPR and, therefore, shall communicate the rectification to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves

Moving to the issue of the evidence on the incorrectness or incompleteness of personal data, it should be noted that while article 16 of the GDPR makes reference to the possibility of the data subject submitting a supplementary statement within the context of the exercise of the right to complete personal data, nothing is said about an obligation of the data subject of proving that the data is incomplete or incorrect.

On this topic, the Advocate General in *case Deldits* mentions that "the (in)accuracy of data, and the need for their rectification, is to be assessed on a case-by-case basis, as a consequence of which the evidence that may be required for that purpose will vary"[15] and that the data subject may be "required to produce evidence that may be reasonably required to establish the inaccuracy of that data in the light of the purposes for which they were collected or processed". However, the data subject does not have to claim or to demonstrate a particular interest in the rectification of inaccurate data, nor has to prove the existence of any harm caused by the inaccuracy of the data.

Consequently, it appears that the evidence to be produced by a data subject within the context of the exercise of the right of rectification may be more or less demanding depending on the case, and while in some cases "it will be sufficient for the data subject to simply request rectification of, for example, the spelling of a name" (European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 220), where the request is linked to "legally significant matters, such as the data subject's legal identity, or the correct place of residence for the delivery of legal documents" (European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 220), the data subject may be required to provide reasonable evidence of the alleged inaccuracy. However, any request of proof made within this context cannot be unreasonable and it cannot be so demanding that it precludes data subjects from having their data corrected or completed.

Additionally, and considering the controllers' obligation of facilitating the exercise of data subjects rights set forth in article 12(2) of the GDPR, it can be argued that any request of proof of the inaccuracy of personal data should not only be reasonable, but also limited to what is necessary and made in such a way that it has the minimum impact possible in the data subject's ability to exercise the right of rectification (for example, by giving the data subject several options for the purpose of providing the requested evidence, so that the data subjects can choose the option that is easier to them, and by not adding any formalities or requirements that are not strictly necessary).

Finally, it should be noted, now regarding the supplementary statement mentioned in article 16 of the GDPR, that the GDPR does not specify that such a statement must comply with any formalities and, therefore, it must be concluded that such statement can be submitted in writing, orally or in any other form available.

---

disproportionate effort, further having to be provided to data subject, upon request, information about the recipients to whom the personal data have been disclosed (Kuner, Bygrave, & Docksey, 2020, p. 496).

[15] Case C-247/23, Deldits, 2024, ECLI:EU:C:2024:747, para. 47.

## 3. STATE OF THE ART IN THE APPLICATION OF THE RIGHT OF RECTIFICATION TO INFERENCES

As it became clear from the last section, while the right of rectification is not new and its wording is apparently quite simple and straightforward, its application is not free of doubts, existing two additional aspects that require clarification, particularly when this right is applied to inferences.[16]

Firstly, as it has been noted, the legal status of inferences as personal data is "marked by inconsistencies and contradictions within and between the views of the Article 29 Working Party and the European Court of Justice" (Wachter & Mittelstadt, 2019, p. 5). Secondly, it is also debated to which extent non-verifiable inferences (such as predictions of development of a disease in the future) may be subject to the right of rectification.

In this section we will explore the different views on these two topics, starting by the analysis of the existing guidelines issued by the WP29 and its successor, the European Data Protection Board (EDPB, hereinafter). We will then move to the analysis of the CJUE case law[17] most relevant for the two topics identified above, concluding this chapter with the analysis of the state of the art in the application of the right of rectification to inferences.

Firstly, and regarding the qualification of inferences as personal data, it is worth recalling that under article 4(1) of the GDPR, personal data means any information relating to an identified or identifiable natural person.

Secondly, it should be noted that the definition above does not differ from the one included in the Data Protection Directive, reason why the opinion of the WP29 on the concept of personal data (Article 29 Data Protection Working Party, 2007) remains relevant. In this respect, it is particularly important to recall the analysis of the four building blocks of the definition of personal data identified by the WP29 and, in particular, the fact that, according to the WP29, "in order to consider that the data "relate" to an individual, a "content" element OR a "purpose" element OR a "result" element should be present" (Article 29 Data Protection Working Party, 2007, p. 10) and that "data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests" (Article 29 Data Protection Working Party, 2007, p. 11),[18] conclusions which are key to the legal status of inferences (Wachter & Mittelstadt, 2019).

Thirdly, it is worth recalling that, according to the WP29, article 16 of the GDPR applies to "both the 'input personal data' (the personal data used to create the profile)

[16] For the purposes of this article, we will consider inferences to be information relating to a data subject that is generated through deduction or reasoning, including predictions, decisions, opinions, and assessments (Wachter & Mittelstadt, 2019).

[17] Considering the scope of this paper, we will focus on cases submitted to the Court of Justice of the European Union, even though there are also several cases ruled by the European Court of Human Rights relevant within this context (Kuner, Bygrave, & Docksey, 2020, p. 472).

[18] For a detailed application of these blocks to inferences see Fischer, 2020.

and the 'output data' (the profile itself or 'score' assigned to the person)" (Article 29 Data Protection Working Party, 2018, p. 17), thus being considered that inferences may qualify as personal data. This was further developed by the EDPB (2023), who argues in its guidelines on the right of access that data inferred from other data, rather than directly provided by the data subject, such as "algorithmic results, results of a health assessment or results a personalization or recommendation process" constitute personal data, conclusion also in line with the EDPB's guidelines on the right to portability (Article 29 Data Protection Working Party, 2017), on which this distinguishes, for the purpose of the exercise of this right, between personal data provided by the data subject (which covers data actively provided by the data subject and observed data) and inferred and derived data, which is not covered by the scope of this right, being mentioned that these categories of data include "personal data that are created by a service provider (for example, algorithmic results)" (Article 29 Data Protection Working Party, 2017, p. 10). In the same vein, the EDPB also noted in its guidelines on the right of access that if a candidate requests access to personal data relating to him or her collected in the course of the recruitment, then the controller shall provide the data subject not only with personal data actively communicated by the data subject, but also with the summary of any interview carried out within this context, including "the subjective comments on the behaviour of the data subject the HR officer wrote during the job interview" (EDPB, 2023).

Finally, reference should be made to the existing guidelines on legitimate interest, in public consultation at the moment of writing, in which it is stated that the right of rectification, a right "of great importance to enable data subjects to have control over their own personal data" (European Data Protection Board, 2024, p. 25), can be invoked regardless of legal basis for processing applicable, being however "especially relevant in situations where the data have not been obtained from the data subject, as the likelihood of inaccuracies and incompleteness is generally higher in such situations" (European Data Protection Board, 2024, p. 25).

Therefore, and considering the above, it is safe to conclude that, according to the existing European guidelines, not only inferences shall be considered personal data, insofar as they relate to a data subject, but also that this is one of the contexts where the right of rectification is more relevant.

As to the second aspect mentioned above, legal doctrine has concluded that the WP29 considered that "opinions and assessments, understood here as inferences, do not need to be objective or verifiable to be considered personal data" (Wachter & Mittelstadt, 2019, p. 28). Nonetheless, it should also be noted that the European Data protection Supervisor (EDPS, hereinafter) stated, in 2014, that the right of rectification "only applies to objective and factual data, not to subjective statements (which, by definition, cannot be factually wrong)" (European Data Protection Supervisor, 2014, p. 18), adding, in relation to non-factual data, that data subjects should be permitted to "complement existing data with a second opinion or counter expertise in such situations, e.g. as regards decisions made during an appeal procedure in disciplinary

cases, or comments on an annual performance appraisal", therefore making a distinction between objective/hard data and subjective/soft data when grating the right of rectification. According to the EDPS opinion, while objective data could be rectified, subjective data could only be completed, considering additionally that in the second case, "to ensure the completeness of a file, data subjects may also ask to add their opinion to it" (European Data Protection Supervisor, 2014).

Furthermore, it should be noted that the EDPB mentioned recently, in its guidelines on legitimate interest, that, "in principle, the right to rectification can be successfully invoked by the data subject only when they can substantiate that the data being processed is objectively incorrect or incomplete" (European Data Protection Board, 2024, p. 25) and that this right cannot be used to make sure that a certain evaluation reflects the personal opinions of the data subject.

While we believe that it can still be interpreted from the above that, following the existing guidelines, it should be considered that non-verifiable inferences are personal data and may be the subject of the right of rectification, provided that this right is used to correct or complete the aforementioned inferences with objective information (and not the data subject's opinion), we believe that the wording used by the EDPB does not, in any way, contribute to a clear understanding about the cases in which the right of rectification may be used. Further, where inferences are made about someone's preferences, the controller may reach the conclusion that a data subject prefers a certain type of music, and the data subject may not agree with it. One can wonder whether this disagreement of the data subject concerns an opinion of him or her, in which case the right of rectification could not be exercised. While we agree with the legal doctrine that sustains that these data on personal preferences are factual, even though they can be more subjective (Custers & Vrabec, 2024), the interpretation from the EDPB mentioned above should be clarified.

Moving to the analysis of relevant case law, in joint cases C-141/12 and C-372/1251 the CJEU was asked to clarify whether the data reproduced in a minute concerning the data subject was personal data within the meaning of Article 2(a) of the Data Protection Directive and if a legal analysis included in the minute constitutes personal data within the meaning of the aforementioned provision. The case related to the exercise of the right of access by data subjects who have applied for lawful residence in the Netherlands and wished to access the document drafted by the relevant authority which contained the legal analysis on whether to grant residence status.

In its conclusions, the Advocate General of the case mentioned that "it became clear that the applicants wished to understand the reasoning underlying the individual decisions on their residence status",[19] considering that "broadening the meaning of the rules governing the protection of personal data or extending their scope to cover opinions and other measures taken during the preparation and investigation prior to

[19] Opinion of Advocate General Sharpston in Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel, 2013, ECLI:EU:C:2013:838, para. 28.

the adoption of a final decision"[20] would not be adequate, and therefore concluding that while the facts in the legal analysis that relate to the data subject (name, date of birth, etc.) were personal data,[21] the legal analysis carried out was not personal data.[22]

In the words of the Advocate General "Personal data and other elements of fact may very well be inputs in the process leading to answering that question; but that does not make the legal analysis itself personal data",[23] being, however, also sustained that subjective analysis could be personal data. Regarding this specific aspect, the Advocate General mentions that:

> Facts can be expressed in different forms, some of which will result from assessing whatever is identifiable. For example, a person's weight might be expressed objectively in kilos or in subjective terms such as 'underweight' or 'obese'. Thus, I do not exclude the possibility that assessments and opinions may sometimes fall to be classified as data.[24]

In the same line, the decision taken by the Court considered that "the legal analysis in a minute (…) although it may contain personal data, it does not in itself constitute such data"[25] and, therefore, such an analysis "is not in itself liable to be the subject of a check of its accuracy by that applicant and a rectification under Article 12(b) of Directive 95/46".[26]

It has been noted by legal doctrine that a legal analysis is comparable to an analysis where new data is inferred, further being highlighted that such analysis "can consist of multiple inferences connected to an identified or identifiable individual (i.e. assessment of how the law applies to a case), leading to a final opinion, result, or inference" (Wachter & Mittelstadt, 2019, pp. 31-32), and concluded that, under the CJEU interpretation, the process for reaching a conclusion would not be personal data. Others have nevertheless sustained a different interpretation, considering that the decision of the Court "can be interpreted as meaning, that the analysis by which inferences are created does not constitute personal data, but inferences that are drawn in the process can constitute 'facts' about *a person*" (Fischer, 2020, pp. 34-35).

Furthermore, regarding the second aspect of our analysis in this section, it has been considered that the Advocate General definition of personal data as "facts about an individual"[27] and the irrelevance of the objectiveness or subjectiveness of the facts suggest the Advocate General "views verifiability as a necessary component of personal data" (Wachter & Mittelstadt, 2019, p. 35).

---

[20] Ibidem, para 32.
[21] Ibidem, paras. 42 and 43.
[22] Ibidem, para. 47.
[23] Ibidem, para. 59.
[24] Ibidem, para. 57.
[25] Judgment of joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel, 2013, ECLI:EU:C:2014:2081, para. 39.
[26] Ibidem, para. 45
[27] Opinion of Advocate General Sharpston in Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel, 2013, ECLI:EU:C:2013:838, para. 56.

Finally, attention has been drawn to the statement made that the purpose of data protection law is not to assess the accuracy of decision-making processes involving personal data (Wachter & Mittelstadt, 2019), as the Court mentions that "extending the right of access of the applicant for a residence permit to that legal analysis would not in fact serve the directive's purpose of guaranteeing the protection of the applicant's right to privacy".[28]

Despite the above being concerning for the matter under analysis, it is worth noting, before moving to our conclusions, that the CJEU was asked afterwards about the matter, presenting some conclusions that, to a certain extent, are not in line with the above.

In fact, in case C-434/16, the CJEU was questioned whether an examination script, including the answers given, was personal data and, therefore, if the examination candidate could exercise is right of access to the script on the basis of the Data Protection Directive.

In this case, the Advocate General considered that the examination script, as well as the corrections made by examiners contained therein, which could classify as inferences, are personal data,[29] interpretation which was also sustained by the Court, who decided that both the answers to an exam and the comments of the examiner to those answers are information relating to the candidate and, therefore, personal data.[30] In the case, the CJEU further added that if other conclusion was reached "that would have the effect of entirely excluding that information from the obligation to comply not only with the principles and safeguards that must be observed in the area of personal data protection",[31] even though, naturally, "the right of rectification provided for in Article 12(b) of Directive 95/46 cannot enable a candidate to 'correct', a posteriori, answers that are 'incorrect'"[32] and "the rights of access and rectification, under Article 12(a) and (b) of Directive 95/46, do not extend to the examination questions, which do not as such constitute the candidate's personal data".[33]

Worth noting is also the statement made by the CJEU that the definition of personal data "potentially encompasses all kinds of information —not only objective but also subjective, in the form of opinions and assessments— provided that it 'relates' to the data subject",[34] thus being considered that opinions and assessments can indeed constitute personal data.

Hence, even though some argue that the CJEU reinforced in this case "their previous opinions in that only limited rights are granted over assessments (e.g. opinions, inferences)" (Wachter & Mittelstadt, 2019, p. 45) and on the purpose of data

[28] Judgment of joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel, 2013, ECLI:EU:C:2014:2081, para. 46.
[29] Opinion of Advocate General Kokott in Case C-434/16, Nowak, 2017, ECLI:EU:C:2017:582, para. 63.
[30] Judgment of case C-434/16, Nowak, 2017, ECLI:EU:C:2017:994, para. 42
[31] Ibidem, para. 49.
[32] Ibidem, para. 52.
[33] Ibidem, para. 58.
[34] Ibidem, para. 34.

protection law, we consider that the decision taken in this second case is a positive step in the alignment between the perspectives of the EDPB and the CJEU on the qualification of inferences as personal data, including those that are subjective or non-verifiable.

In fact, it can be concluded that while it appears to exist some level of contradiction between existing guidelines and case law, which was particularly evident before the *Nowak case*, and while we understand why this lead authors to sustain that a new data protection right, the "right to reasonable inferences" (Wachter & Mittelstadt, 2019, p. 2), comprised by an *ex-ante* justification to establish whether an inference is reasonable and an *ex-post* mechanism enabling unreasonable inferences to be challenged, was necessary to close the accountability gap (Wachter & Mittelstadt, 2019), we are of the opinion that the most recent case law on this matter as contributed to close the gap in the understanding that inferences can be considered personal data. Furthermore, by mentioning that the definition of personal data encompasses objective and subjective information, it can be concluded that the subjectiveness of a certain information does not affect its qualification as personal data. However, the Court was not clear regarding to which extent a subjective analysis can be completed, rather focusing on objective data that could be rectified and in the fact that information such as answers to an exam cannot be rectified.

Finally, while we understand that the CJEU's opinion that the goal of data protection law is not to guarantee the accuracy of decision-making may be seen as worrying, we believe that the interpretation of this Court could be narrowly interpreted, being solely considered that data protection law should not be used to access documents. However, insofar as personal data is included in those documents, access to that data should be provided and, furthermore, access to the documents should also be granted insofar as they are essential to enable the data subject to exercise the rights set forth the GDPR, including the right of rectification (AEPD, 2020).

## 4. RIGHT OF RECTIFICATION AND AI SYSTEMS – APPLICABILITY AND SPECIFIC CHALLENGES

Many AI systems process personal data and, as it has been noted, personal data may be processed throughout the lifecycle of an AI system, from the training phase (covering activities such as the definition and categorization of datasets and data cleansing), to the validation, deployment and operation of AI systems (AEPD, 2020).

Furthermore, as noted in recital 12 of the AI Act, a key characteristic of AI systems is their capability to infer, this referring to the "process of obtaining the outputs (…) which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data", thus generating inferences, including those which are non-intuitive and unverifiable (Wachter & Mittelstadt, 2019), carrying a risk of being incorrect or discriminatory, potentiating existing or new bias (Sartor, 2020).

Where inferences are drawn by an AI system, a distinction must be made between general correlations learned by the AI system and the results of applying the defined correlations to a data subject (Sartor, 2020). The correlations learned will not, in principle, include personal data (even though the same may not be true for the process of establishing those correlations). However, when they are applied to a data subject, the inference relates to the data subject, reason why they should, as we have seen above, be qualified as personal data. Nonetheless, as it has been noted, it may be hard to determine exactly when these correlations apply to specific data subjects, being therefore considered personal data (Custers & Vrabec, 2024).

Furthermore, while it is not discussed that where certain parameters are applied to information relating to a data subject (referred to as input data), this information is personal data, and further being established that the output of this process may also be personal data, the existence of intermediate inferences (Sartor, 2020) and their qualification as personal data deserve further attention.

In fact, it is worth recalling that existing case law from the CJEU does not seem to support the use of the right of rectification to processes involved in the reasoning behind a decision and, therefore, it does not appear to support the application of the right of rectification to the logic behind the inferred data (Custers & Vrabec, 2024).

However, as it has been highlighted by legal doctrine, in some cases it is almost impossible for the data subject to assess if a certain inference is correct. As mentioned, if "a data controller assesses that a data subject has 75 % probability of attracting cancer in the next five years, the data subject cannot assess whether that is correct" (Custers & Vrabec, 2024, pp. 9-10). Still, as correctly noted, in these cases the data subject could possibly assess whether the application of the correlations used to reach the final output are correct. In other words, at least in some cases, there could be certain intermediate inferences which are verifiable and could be corrected. As an example, the afore mentioned probability of attracting cancer could be based on factors such as habits or the inclusion in a certain group with elevated risk which were incorrectly attributed to the data subject.

Nonetheless, these intermediate inferences are part of the reasoning behind a decision and, according to the CJEU, such analysis would not constitute personal data, even though, if these intermediate inferences were considered alone, their result would, as we have seen above, constitute personal data, as they would each be an inference relating to the data subject.

Therefore, one of the challenges that can be clearly identified herein relates to the existence of intermediate inferences made through automated means (in the case, AI systems) which appear to be outside the scope of data protection law.

However, there are other challenges that should also be highlighted. As we have seen, while some inferences made by AI systems are verifiable, this meaning its correctness may be objectively determined, others are non-verifiable, in the sense that they are probabilistic or otherwise not objectively determined (Sartor, 2020), and while in the first set of inferences the exercise of the right of rectification is

straightforward, the same cannot be said for non-verifiable inferences. In fact, even though, as we have seen, the fact that an inference is non-verifiable should not affect its qualification as personal data, the extent to which the right of rectification may be exercised over these inferences remains unclear, as it appears that, in such cases, the data subject would only have the right to complete the personal data used to reach that inference.

Furthermore, as it has been noted, since data analytics often makes use of statistics, these inferences may, and will often, contain error margins (Custers & Vrabec, 2024). Consequently, while an inference of this type may lead to an incorrect result attributed to a data subject, the controller may argue that the inferred data is statistically correct (Custers & Vrabec, 2024), in which case, and following our conclusions in the previous sections, it is not clear if the interpretation of the controller should prevail.

Additionally, cases may exist where there is no error in the input data or in the sequence of inferences made for example about someone's preferred music genre and still the data subject considers that the output of the analysis is incorrect (Custers & Vrabec, 2024). Again, in these cases, it is not clear whether the data subject's opinion should prevail or if the controller can maintain the inference made, considering that this is neither incorrect nor incomplete.

Finally, even if all of the challenges mentioned above are surpassed, there are still practical hurdles that have to be considered, particularly those derived from the opacity of certain AI systems, which may reduce accountability of their 'owners' and the contestability of the decisions taken (Hildebrandt, 2016). In fact, even if, from a legal point of view, it is considered that intermediate inferences are personal data and may be the subject of a right of rectification, the fact remains that the way how some AI systems reach a decision is not transparent (this giving rise to the use of the notion of "black-box" AI (Bathaee, 2018)). Furthermore, the fact that information gets subsumed by an AI model in formats that are illegible to most people (being given the example of language models, in which individual words are not stored as strings of text, but rather as represented as numerical vectors derived from the model's training) has also been identified as a challenge for both understanding (Gucluturk, 2024) and updating or deleting the data stored in these models (European Data Protection Supervisor, 2024). These are challenges faced by controllers which do not relate to the right of rectification specifically, but rather to, in general, the application of data subject rights in the context of AI.

Nevertheless, these challenges are also felt by data subjects since, as it has been noted, it "will be difficult to contest an automatic decision without a clear explanation of the decision reached (Roig, 2017, p. 6). In fact, even though the information rights set forth in articles 13 and 14 of the GDPR can help data subjects understand when and what inferences are drawn, this right and the "right to explanation" derived by authors

form the GDPR,[35] as well as article 86 of the AI Act, under which any affected person subject to a decision taken based on the output from a high-risk AI system shall have the right to obtain "clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken", appear to be insufficient to guarantee that data subjects are provided with clear information on how AI systems make inferences about them and in which cases intermediate inferences that may qualify as personal data exist.

## 5. RIGHT OF RECTIFICATION AND AI SYSTEMS – POSSIBLE SOLUTIONS

Having identified at least some of the challenges encountered when applying the right of rectification to inferences and, specifically, inferences made by AI systems, we will explore in this final section how could some of these be surpassed, either by the action of competent authorities or by measures to be implemented by controllers.

In fact, it has been noted that "AI systems must guarantee privacy and data protection throughout a system's entire lifecycle", this covering not only the information initially provided by data subjects, but also the information generated about that data subject (High-Level Expert Group on AI, 2019), as well as the model itself, if this included "inaccurate personal data of third data subjects that are able to be reidentified and thus associated to them wrong information" (AEPD, 2020). However, despite being noted that data subject rights must be respected regardless of the AI approach or the technical architecture chosen (EDPB-EDPS, 2021), the fact remains that this will only be possible if it is clear, for both controllers and data subjects, when and to which extent these rights may be exercised. In fact, and focusing on the right of rectification, this may play a key role in mitigating the impact of error rates in AI systems if its effective exercise is ensured.

Among the actions by competent authorities that are required to ensure the effective exercise of the right of rectification over inferences made by AI systems, we highlight the need of issuing guidelines in which it is clarified to which extent this right applies to intermediate inferences (which do not appear to have characteristics that would differentiate them from final inferences in such a way that these should not be qualified as personal data) and what is the exact scope of the right of rectification when applied to non-verifiable inferences. In particular, it should be clarified whether, in these cases, only the right to complete personal data may be exercised, the data subject having the right to provide specific additional data that support a different conclusion

[35] The "right to an explanation" has been derived from the combination (i) of the information obligations on automated decision-making, including profiling, included in articles 13 and 14 of the GDPR (in terms of information provided ex ante) and in article 15 (within the context of the exercise of the right of access), (ii) with the safeguards against automated decision-making covered by article 22(3) and the reference, in recital 71 of the GDPR, to the right of obtaining specific information and an explanation of the decision reached as part of those safeguards. However, there is still an ongoing discussion on the existence and scope of this right. See Malgieri, 2019; Malgieri & Comandé, 2017 and Wachter, Mittelstadt, & Floridi, 2017.

from the one reached by the AI system. Furthermore, it should be clarified which obligations fall upon the controller when this does not agree with the opinion of the data subject that the inference reached is incorrect and, specifically, it should be clear in which cases the controller may decide to maintain an inference because it considers that this is correct. Finally, any derogations to the exercise of rights on datasets or on the AI systems should be identified and densified (CNIL, 2024).

At the same time, there is clearly work to be done regarding the interpretation of the transparency requirements set forth in the GDPR, to ensure that, in general, data subjects are generally able to exercise their rights over personal data processed within the context of AI systems. Regarding this aspect, it should be clear that as inferences (both intermediate and final) are personal data, these should be identified in the categories of personal data processed described in the documents aimed at complying with article 14 of the GDPR and be part of the information provided when a data subject exercises the right of access. Furthermore, it could be sustained that as access to the documents should be granted insofar as they are essential to enable the data subject to exercise the rights set forth the GDPR, so should access to the process followed by the AI system to reach a final inference be granted, to that extent this is needed to understand the intermediate inferences made in order to reach that final inference or decision. This way, even if the final inference reached is non-verifiable, data subjects would be able to assess if such inference is based on one or more intermediate inferences which are verifiable and contest them directly.

As to the good practices that may be implemented by controllers in order to facilitate and correctly manage the exercise of data subject rights, including the right of rectification, within the context of AI, there are several measures that can be implemented.

Firstly, controllers should, when developing an AI system "be aware from the system design stage that they must include appropriate mechanisms and procedures for responding to requests that may be received" (CNIL, 2022). In this context, controllers should assess which measures are adequate, which may include managing datasets in a way that allows traceability of their use (European Data Protection Supervisor, 2024); keeping a traceable record of the processing of personal data carried out within the context of the development and use of the AI system; identifying to which extent the personal data processed is part of mixed datasets, in which case "it may be useful to differentiate between mixed datasets in which personal and nonpersonal data are inextricably linked and those in which this is not the case" (European Data Protection Board, 2023, p. 34); identifying when are inferences made, irrespective of whether these are solely intermediate inferences or the final output produced by the AI system; and identifying which of those inferences are verifiable or non-verifiable. To support this assessment, tools as the data protection impact assessment set forth in article 35 of the GDPR, which may be mandatory under this regulation, appear to be of great assistance.

Likewise, where the AI system is provided by a third-party, adequate due diligence should be undertaken, this including a review of the measures, from those listed above and others deemed necessary, which were or can be applied to the AI system.

Furthermore, where non-verifiable inferences are produced, controllers can identify in their records that they consider these inferences to be subjective (Ustaran, 2019), further detailing aspects such as error margins, how the opinion is reached, and to which extent these inferences are based in intermediate verifiable inferences.

Moreover, to mitigate the risk of incorrect inferences, controllers should critically check the results generated by AI systems for accuracy and discrimination, that way actively identifying incorrect inferences and reducing its number.

If data subjects exercise their right of rectification on inferences made by AI systems, controllers should take reasonable steps to verify the accuracy of the personal data in question, considering the arguments and evidence provided by the data subject (ICO, s.d.), as well as the measures already in place to verify, in general, the accuracy of the outputs produced by the AI model. Also, and as general guidance, controllers should consider that the more important it is that the personal data is accurate, the greater the effort that the controller should make in order to check the accuracy of the contested inferences (ICO, s.d.).

Additionally, still within the context of the management of the exercise of the right of rectification, controllers should consider if, despite not being completely proven by the data subject that the contested personal data are inaccurate, it seems reasonable, from the controller's point of view, to honour the data subject's request (Ustaran, 2019), and, where that is the case, the request should be honoured. In fact, many times, such as in the case of predictions about the data subject's interests, it will be in both the interest of the controller and the data subject to correct the inference made (Custers & Vrabec, 2024), even if this is, for example, statistically correct.

Where the controller considers that the personal data is not incorrect and should not be corrected, the data subject should be given the option to complete the personal data at stake, and the controller should have the information provided into consideration, recording the analysis of the further information provided that was made. Furthermore, the data subject should be informed of the reasons why the controller considers the personal data to be correct and of his or her right to make a complaint to the relevant supervisory authority and to seek judicial remedy, as required under article 12(4) of the GDPR. Controllers could also, as a good practice, place a note on their system indicating that the data subject has challenged the accuracy of the data, and the reasons presented for doing so (ICO, s.d.).

Finally, when the controller still has the training data, re-training the model should also be considered, "whenever it is not disproportionate to the rights of the controller, in particular the freedom to conduct a business" (CNIL, 2024).

## 6. CONCLUSION

As we have seen, the right of rectification, comprised by the rights of correcting and completing personal data, faces many challenges when applied to inferences, particularly those generated by AI systems.

The apparent discrepancies between the CJEU's and the EDPB's views on the qualification of inferences as personal data, as well as the doubts regarding the extent to which the right of rectification may be exercised over non-verifiable inferences and the CJEU's opinion that the remit of data protection law is not to guarantee the accuracy of decision-making processes, are only exacerbated when inferences are made by AI systems, which may not only make non-intuitive and non-verifiable final inferences, but also make, during the process leading to the final inference relating to a data subject, several intermediate inferences whose legal qualification as personal data and possibility of being questioned are not clear.

In this article, we argue that intermediate inferences, insofar as they relate to a data subject, thus not presenting a material difference from final inferences, should be qualified as personal data and data subjects should be able to challenge them. Furthermore, having concluded that the extent to which the right of rectification may be exercised over non-verifiable inferences is not clear, we argue that competent authorities should clarify if, in these cases, only the right to complete personal data can be exercised. We also note that by recognizing that intermediate inferences can be personal data, data subjects may be able to contest intermediate verifiable inferences that have a direct impact on a final non-verifiable inference, thus reducing the limitations recognized to the right of rectification where the final inference at stake is non-verifiable. We highlight the importance of clarifying what are the obligations that fall upon the controller when it does not agree with the data subject's allegations that and inference is not correct and in which cases the controller may, in these situations, decide to maintain an inference because it considers that this is correct.

Finally, we identify a set of measures that may be implemented by controllers to facilitate and manage the exercise of the right of rectification in the context of inferences made by AI systems, from measures relating to the traceability of the personal data processed within the context of the development and use of an AI system and the traceability of the processing carried out and the inferences made by the AI system, to measures that may be implemented when the controller faces the exercise of the right of rectification over an inference made by an AI system.

We consider that the right of rectification can indeed play a very relevant role in correcting errors made by AI systems and, therefore, can aid in protecting data subjects against incorrect inferences made by those systems. However, the effectiveness of this right in the context of AI largely depends on competent authorities clarifying how and to which extent this right may be exercised, and identifying the measures taken by controllers to facilitate its exercise. The implementation of these measures by relevant controllers is also crucial, and only the action of both relevant

authorities and controllers can ensure that the right of rectification is not lost when its application is translated to AI systems.

## 7. BIBLIOGRAPHY

Agencia Española de Protección de Datos (2020). *GDPR compliance of processings that embed Artificial Intelligence An introduction*. https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf

Article 29 Data Protection Working Party. (2007). *Opinion 4/2007 on the concept of personal data*. Adopted on 20th June. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Article 29 Data Protection Working Party. (2017). *Guidelines on the right to "data portability"*. https://ec.europa.eu/newsroom/article29/items/611233

Article 29 Data Protection Working Party. (2018). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/612053/en

Bathaee, Y. (2018). The artificial Intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, *31*(2), pp. 889-938. https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf

CNIL (2022). *AI: ensuring GDPR compliance*. https://www.cnil.fr/en/ai-ensuring-gdpr-compliance

CNIL (2024). *Respect and facilitate the exercise of data subjects' rights*. https://www.cnil.fr/en/respect-and-facilitate-exercise-data-subjects-rights

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *Council of Europe. European Treaty Series* – No. 108. Strasbourg, 28.1.1981. https://rm.coe.int/1680078b37

Custers, B., & Vrabec, H. (2024). Tell me something new: data subject rights applied to inferred data and profiles. *Computer Law & Security Review*, *52*. https://www.sciencedirect.com/science/article/pii/S0267364924000232

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *OJ L 281, 23.11.1995*. http://data.europa.eu/eli/dir/1995/46/oj

Egan, M. (2024, March 12). AI could pose 'extinction-level' threat to humans and the US must intervene, State Dept.-commissioned report warns. *CNN*. https://edition.cnn.com/2024/03/12/business/artificial-intelligence-ai-report-extinction/index.html

European Commission. (2018). *Communication from the Commission - Artificial Intelligence for Europe. European Commission* (COM (2018) 237 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018DC0237

European Commission. (2020). *White Paper on Artificial Intelligence - A European approach to excellence and trust* (COM(2020) 65 final). https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission. (2021). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts* (COM/2021/206 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

European Commission. (2024). *Artificial Intelligence – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683

European Council. (2017). *Council meeting (19 October 2017) – Main results* https://www.consilium.europa.eu/en/meetings/european-council/2017/10/19-20/#:~:text=EU%20leaders%20agreed%20that%20their,results%20and%20should%20be%20consolidated.

European Data Protection Board (2021). *EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

European Data Protection Board. (2023). *Guidelines 01/2022 on data subject rights - Right of access.* https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

European Data Protection Board. (2024). *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en

European Data Protection Supervisor. (2014). *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data*. https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf

European Data Protection Supervisor. (2024). *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems*. https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf

European Union Agency for Fundamental Rights & Council of Europe. (2018). *Handbook on European data protection law*. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

Fischer, C. (2020). *The legal protection against inferences drawn by AI under the GDPR*. Tilburg University. https://arno.uvt.nl/show.cgi?fid=151926

Gucluturk, O. (2024). *How to handle GDPR data access requests in AI-driven personal data processing*. OECD.AI Policy Observatory. https://oecd.ai/en/wonk/gdpr-data-access-requests

Gutiérrez, J. D. (2024). *Consultation paper on AI regulation: emerging approaches across the world*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000390979

High-Level Expert Group on AI. (2019). *Ethics guidelines for trustworthy AI. European Commission*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Hildebrandt, M. (2016). *The New Imbroglio – Living with Machine Algorithms. The Art of Ethics in the Information Society*. https://mediarep.org/bitstreams/76090e54-9c2f-4334-af44-fa1c04db85d0/download

ICO (s.d.). *The right to rectification*. https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/the-right-to-rectification/

Judgment of the Court (Second Chamber) of 20 December 2017. Peter Nowak v Data Protection Commissioner. Request for a preliminary ruling from the Supreme Court. Case C-434/16. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0434

Judgment - 13/03/2025 – Deldits. Case C-247/23. https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-247/23

Judgment of the Court (Third Chamber), 17 July 2014. Joined Cases C-141/12 and C-372/12. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0141

Kuner, C. (et al.) (eds.). (2020). *The EU General Data Protection Regulation (GDPR) A commentary*. Oxford Univerity Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839645

Malgieri, G. (2019). Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations. *Computer Law & Security Review*, *35*(5). https://doi.org/10.1016/j.clsr.2019.05.002

Malgieri, G., & Comandé, G. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law*, *7*(4), pp. 243–265. https://doi.org/10.1093/idpl/ipx019

Marr, B. (2023, June 2). The 15 Biggest Risks Of Artificial Intelligence. *Forbes*. https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/

McKinsey Analytics. (2019). *Global AI Survey: AI proves its worth, but few scale impact*. https://www.mckinsey.com/%7E/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Global%20AI%20Survey%20AI%20proves%20its%2

0worth%20but%20few%20scale%20impact/Global-AI-Survey-AI-proves-its-worth-but-few-scale-impact.pdf

Opinion of Advocate General Sharpston in Joined Cases C-141/12 and C-372/12, YS v Minister voor Immigratie, Integratie en Asiel, 2013. https://curia.europa.eu/juris/document/document.jsf?docid=145566&doclang=EN

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe Treaty Series – No. 223. Strasbourg 10.X.2018. https://rm.coe.int/16808ac918

Roig, A. (2017). Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). *European Journal of Law and Technology*, *8*(3). https://www.ejlt.org/index.php/ejlt/article/view/570

Sartor, G. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530

Singla, A., (et al.) (2024). *The state of AI in early 2024: Gen AI adoption spikes and starts to generate value*. Quantum Black A by McKinsey. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

Ustaran, E. (2019). *European Data Protection Law and Practice* (2nd ed.). International Association of Privacy Professionals. https://pdfcoffee.com/ism-european-data-protection-2nd-edition-4-pdf-free.html

Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 2019(2). https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3409269_code2455045.pdf?abstractid=3248829.&mirid=1

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection *Regulation. International Data Privacy Law*, *7*(2). https://doi.org/10.1093/idpl/ipx005

Wiewiórowski, W. (2024a). *International Organisations Workshop on Data Protection. European Data Protection Supervisor*. https://www.edps.europa.eu/system/files/2024-09/ios_ws_washington_23_septermber_24_speech_ww_fin_formatted_en.pdf

Wiewiórowski, W. (2024b). *Speech - Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) Autumn Conference. European Data Protection Supervisor*. https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/2024-10-16-speech-berufsverband-der-datenschutzbeauftragten-deutschlands-bvd-autumn-conference_en